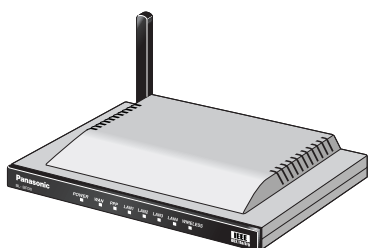
Panasonic®

取扱説明書

カメラコントロールユニット
（IPv6／VPN対応無線ルーター）

品番 **BL-BR30**

このたびは、カメラコントロールユニットをお買い上げいただき、まことにありがとうございました。

保証書別添付

■ 取扱説明書をよくお読みのうえ、正しくお使いください。
特に「安全上のご注意」（8〜11ページ）は、ご使用前に必ずお読みいただき、安全にお使いください。お読みになったあとは、保証書と一緒に大切に保管し、必要なときにお読みください。
■ 保証書は、「お買い上げ日・販売店名」などの記入を必ず確かめ、販売店からお受け取りください。

特　長

本製品は、以下の特長をもつカメラコントロールユニットです。

■ IPv6対応

インターネットの次世代プロトコルであるIPv6に対応しました。IPv6に対応することで、豊富なグローバルアドレス、IPsecに対応することによるセキュリティの向上、といったメリットを享受することができます。

※ 接続確認済みのIPv6サービス対応プロバイダーについては、パナソニックのサポートウェブサイト（http://panasonic.co.jp/pcc/products/hnetwk/support/）を参照してください。

■ VPN機能

VPNとしてPPTP（IPv4）、IPsec（IPv6）に対応しています。VPNで安全にインターネットを使った通信をすることができます。本製品に接続したカメラの画像データやパソコンのデータを暗号化して送信するので、セキュリティを確保することができます。

■ リピーター機能(中継機能)により無線ネットワーク機器の設置範囲を拡大

本製品と無線LAN機器の間に当社製無線LANアダプター「BL-WA30」（別売品）(以下、無線LANアダプターという)を設置することにより、より広い範囲や電波が届きにくい場所に中継できるようになります。

■ IEEE 802.11a/b/g(切替)対応の高速無線LAN

2.4 GHz 54 Mbps※ (IEEE 802.11g)、2.4 GHz 11 Mbps※ (IEEE 802.11b)、5.2 GHz 54 Mbps※ (IEEE 802.11a)を切り替えて使用できます。802.11gモードは802.11g専用モードと、802.11gと802.11bが同時に使えるモードの2種類を設定できます。また、無線LAN機能の停止もできます。

※ 表示の数値は、無線LAN規格の理論上の最大値であり、実際のデータ転送速度を示すものではありません。

■ 高速スループット

有線WAN－LAN間が最大98 Mbps（IPv4／SmartBits)、最大72 Mbps（IPv6／SmartBits)、最大16 Mbps (FTP [PPTP])とFTTHにも対応できる仕様です。

■ インターネットかんたん設定

本製品には「かんたん設定」機能があります。ウィザードに従って設定するだけで、ウェブブラウザで簡単にインターネット接続の設定ができます。特別なソフトのインストールは不要です。フレッツ、Yahoo! BBなどのプロバイダーを選び、ガイダンスに従った簡単な操作で、インターネット接続ができます。

■ 無線おまかせってい (セキュリティ設定含む)

当社製無線LANアダプター「BL-WA30」（別売品）の各種設定を自動的に行います。その際、無線のセキュリティ設定も自動で行いますので、より確実な無線LANを実現します。

特　長

■ カメラおまかせってい (セキュリティ設定含む)

当社製ホームネットワークカメラ「BL-C10（パン／チルト)、BL-C30（パン／チルト・無線)」(別売品)と組み合わせて利用することにより、無線のセキュリティ設定(暗号化[WEP]設定など)およびカメラのネットワーク関連設定(ポートフォワーディング設定など)を自動的に行うことができるカメラ自動登録機能に対応しています。

■ カメラモニター機能

当社製ホームネットワークカメラ(別売品)と組み合わせて利用することにより、最大16台までのカメラ名と静止画像をモニタリング画面上に一覧表示することができるカメラモニター画面に対応しています。また、このカメラモニター画面の設定も自動的に行うことができます。

※ パナソニックのサポートウェブサイト(http://panasonic.co.jp/pcc/products/hnetwk/support/)には、本書に記載している内容以外にも、さまざまな最新の技術情報などを掲載しております。

【略称について】

- Windows® XPの正式名称は、Microsoft® Windows® XP ProfessionalまたはMicrosoft® Windows® XP Home Editionです。（以下、Windows XPという）
- Windows® 2000の正式名称は、Microsoft® Windows® 2000 ProfessionalまたはMicrosoft® Windows® 2000 Serverです。（以下、Windows 2000という）
- Windows® Meの正式名称は、Microsoft® Windows® Millennium Edition Operating Systemです。（以下、Windows Meという）
- Windows® 98SEの正式名称は、Microsoft® Windows® 98 Second Edition Operating Systemです。（以下、Windows 98SEという）
- UPnPは、Universal Plug and Playの略称です。
- IGDとは、UPnP™フォーラムで定義されたInternet Gateway Deviceを意味します。
- 本書では、「IEEE802.11a」、「IEEE802.11b」、「IEEE802.11g」を、それぞれ、「802.11a」、「802.11b」、「802.11g」と表記しています。
- 本書では、「CATVモデム」または「ADSLモデム」のことを「モデム」と表記しています。
- 本書では、「ホームネットワークカメラ」のことを「カメラ」と表記しています。
- 本書では、「アプリケーションプログラム」のことを「アプリケーション」と表記しています。

【商標／登録商標について】

もくじ

名前や機能の名称からページを探すときは、
「さくいん」が便利です（☞ 184～185ページ）

ご使用の前に

はじめに 6
- 本書に使用しているマークについて 6
- 必要なシステム 6
- 本体と付属品 7

安全上のご注意 8

正しくお使いいただくためのお願い 12

セキュリティに関するご注意 14

各部のなまえ 17
- 正面 17
- 背面 17
- インジケーター 18

アクセスする

機能を知る 19
- トップページ 19
- かんたん設定 21
- 詳細設定 23
- IPv6設定 25
- カメラモニター画面 26

各機能を使う

機能を使う 31
- IPv4接続のプロバイダーを登録する 31
- IPv6接続のプロバイダーを登録する 44
- インターネットへの接続を確認する 56
- 接続設定を管理する 57
- カメラを使う 63
- カメラを自動登録する（カメラおまかせってい） 64
- 無線LANを使う 69
- みえますねっとを使う 79

拡張機能を使う 81
- インターネットから本製品にアクセスする 81
- IPv4接続でセキュリティを強化する 95
- IPv6接続でセキュリティを強化する 101
- IPv4接続でのオプション機能を使う 107
  - · IPアドレス（LAN側）DHCPサーバー 108
  - · PPPoE 110
  - · DNSリレー 110
  - · MTUサイズ 111
  - · ルーティング 111
  - · UPnP 113
  - · IPアドレス通知 115
- IPv6接続でのオプション機能を使う 116
  - · IPv6アドレス（LAN側）RA 117
  - · リンクMTUサイズ 118
  - · ルーティング 118
- VPN（PPTP）を使う 120
- VPN（IPsec）を使う 122

もくじ

各機能を使う

管理する 128
- パスワードを変更する 128
- バージョンアップする 129
- バックアップする 131
- 再起動する 132
- 初期化する 132
- PPPoE接続／切断を使う 133
- VPN（IPsec）接続／切断を使う 134
- ネットワークの接続を確認する 135

情報を知る 136
- ネットワーク情報を知る 136
- 各種ログを知る 139
- サポートを使う 143
- ヘルプを使う 143

その他

初期化 144
- 初期化 (CLEAR SETTINGボタンを使用) 144
- 再起動 144

パソコンのUPnP™設定 145

パソコンのIPv6設定 150
- Windows XPにIPv6アドレスを設定する 150
- IPv6グローバルアドレスを再取得する 153
- IPv6グローバルアドレスを固定で設定する 153

VPN使用時のPPTP設定: Windows XPの場合 154

プロキシサーバー使用時のウェブブラウザの設定 157

パソコンのIPアドレスやMACアドレスを確認するには 158
- Windows XP／2000の場合 158
- Windows Me／98SEの場合 158

パソコンのIPアドレスを固定するには 160
- Windows XP／2000の場合 161
- Windows Me／98SEの場合 163

工場出荷時設定一覧 165

用語解説 170

仕様 179

保証とアフターサービス 182

さくいん 184

はじめに

本書に使用しているマークについて

- ……… 参照するページを示します。
- ……… 操作上お守りいただきたい重要事項や禁止事項が書かれています。必ずお読みください。
- ……… 便利な使いかたやアドバイスなどの関連知識を記載しています。

必要なシステム

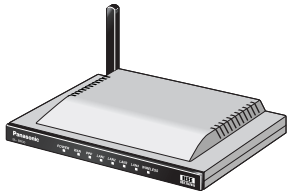
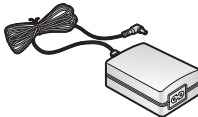
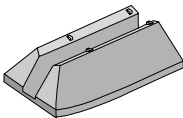
項目	概要
OS(IPv6)	Windows® XP
OS(IPv4)	Windows® XP、Windows® 2000、Windows® Me、Windows® 98SE
インターフェース	10／100 MbpsのLANカードが内蔵されていること
メモリー	64 MB以上
プロトコル	TCP／IPプロトコルがインストールされていること
ウェブブラウザ	Internet Explorer 6.0以降（日本語版）

使用しているパソコンについて不明な点がありましたときは、お客様ご相談センターでは対応しかねますので、直接パソコンメーカーにお問い合わせください。

■ 当社対応製品 (別売品) (平成16年12月現在)

ホームネットワークカメラ

屋内タイプ

BL-C30　(パン／チルト・無線)
BL-C10　(パン／チルト)

無線LANアダプター

BL-WA30

本体と付属品

ご使用いただく前に、本体と付属品を確認してください。
万一、不備な点がありましたら、お手数ですがお買い上げの販売店までご連絡ください。

□ 本体....................................1台	□ ACアダプター..................1個 (コード長　約1.8 m) (☞ かんたんガイド)	□ イーサネットケーブル （カテゴリー5ストレート ケーブル）※.......................1本 (ケーブル長　約1 m) (☞ かんたんガイド)
□ スタンド............................1個 (☞ かんたんガイド)	□ ACコード........................ 1本 (コード長　約55 cm) (☞ かんたんガイド)	※ 付属のイーサネットケーブルは本体とパソコンとの接続用です。モデム(またはONU)との接続には、別途イーサネットケーブル(市販品)が必要です。

□ かんたんガイド..........1部
□ ご使用の前に／困ったときには..........1冊
□ CD-ROM (取扱説明書、設定ガイド)..........1枚
□ 保証書.......... 1式
□ 注意ラベル..........1枚
□ ご愛用者登録のお願い..........1枚

安全上のご注意　必ずお守りください

お使いになる人やほかの人への危害、財産への損害を未然に防止するため、必ずお守りいただくことを、次のように説明しています。

■ **表示内容を無視して誤った使いかたをしたときに生じる危害や損害の程度を、次の表示で区分し、説明しています。**

警告	この表示の欄は、「死亡または重傷などを負う可能性が想定される」内容です。
注意	この表示の欄は、「傷害を負う可能性または物的損害のみが発生する可能性が想定される」内容です。

■ **お守りいただく内容の種類を、次の絵表示で区分し、説明しています。**
（下記は絵表示の一例です。）

🛇	このような絵表示は、してはいけない「禁止」内容です。
❗	このような絵表示は、必ず実行していただく「強制」内容です。

⚠ 警 告

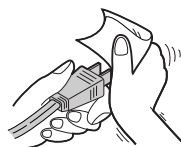
ACコードやプラグを破損するようなことはしない

ドアにはさみ込んだり、傷つけたり、加工したり、熱器具に近づけたり、無理に曲げたり、ねじったり、引っぱったり、重い物を載せたり、束ねたりしない。

禁　止

傷んだまま使用すると、感電・ショート・火災の原因になります。

- コードやプラグの修理は、販売店にご相談ください。

ACコードのプラグのほこりなどは定期的にとる

プラグにほこりなどがたまると、湿気などで絶縁不良となり、火災の原因になります。

- ACコードのプラグをコンセントから抜き、乾いた布でふいてください。

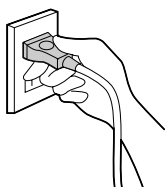
ぬれた手でACアダプターやACコードの抜き差しはしない

ぬれ手禁止

感電の原因になります。

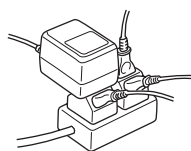
安全上のご注意　必ずお守りください

⚠ 警告

ACコードのプラグは根元まで確実に差し込む

差し込みが不完全ですと、感電や発熱による火災の原因になります。

- 傷んだプラグ・ゆるんだコンセントは使用しないでください。

コンセントや配線器具の定格を超える使いかたや、交流100 V以外での使用はしない

禁　止

たこ足配線などで、定格を超えると、発熱による火災の原因になります。

専用のACアダプター（極性統一形プラグ）以外は使わない

禁　止

専用以外のACアダプターを使用すると、電圧や＋－の極性が異なっていることがあるため、発煙・火災の恐れがあります。

ACコードのプラグを抜き差しするときはプラグ（金属でない部分）を持つ

感電の原因になります。

心臓ペースメーカーの装着部位から22 cm以上離す

電波によりペースメーカーの作動に影響を与える場合があります。

自動ドア、火災報知器などの自動制御機器の近くには設置しない

禁　止

本製品からの電波が自動制御機器に影響を及ぼすことがあり、誤動作による事故の原因になります。

医用電気機器の近くでの設置や使用をしない

手術室、集中治療室、CCU※などには持ち込まないでください。

禁　止

本製品からの電波が、医用電気機器に影響を及ぼすことがあり、誤動作による事故の原因になります。

※CCUとは、冠状動脈疾患監視病室の略称です。

安全上のご注意　必ずお守りください

⚠ 警告

本製品やACアダプターから煙・異臭・異音が出たり、落下などにより破損したときは使用を中止する

そのまま使用すると、火災や感電の原因になります。

● ACアダプターを抜いて販売店へご相談ください。

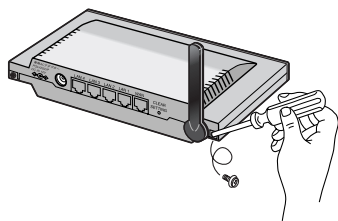
本製品およびACアダプターをぬらさない

水ぬれ禁止

近くに花びん、コップなどを置かないでください。
発火・感電の原因になります。

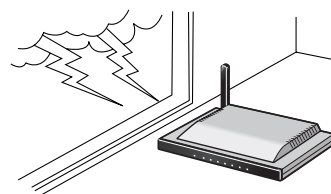
● ぬらした場合は、ACアダプターを抜いて販売店へご相談ください。

絶対に分解したり、修理・改造をしない

分解禁止

故障したり火災・感電の原因になります。

● 修理は販売店へご相談ください。

雷が鳴ったら本製品やACアダプターに触れない

接触禁止

感電の原因になります。

⚠ 注 意

水平でない場所や振動の激しい場所には設置しない

禁　止

落下により、けがの原因になることがあります。

火気を近づけない

火気禁止

火災の原因になることがあります。

水、湿気、ほこり、油煙などの多い場所（調理台や加湿器のそばなど）に設置しない

禁　止

感電・ショートや故障の原因になることがあります。

長期間使用しないときや、お手入れするときは、必ずACコードのプラグをコンセントから抜く

電源プラグを抜く

漏電・感電の原因になることがあります。

CD-ROMは、オーディオ用CDプレーヤーでは絶対に再生しない

禁　止

大音量によって耳に障害を与えたり、スピーカーを破損する恐れがあります。

ケーブルを引っぱったり、コネクター部やアンテナ部に無理な力を加えない

禁　止

損傷や感電の原因になることがあります。

正しくお使いいただくためのお願い

長時間直射日光のあたるところや、冷・暖房器の近くなどに設置しないでください。
（変形・変色または故障・誤動作の原因になります。）

本製品は、涼しくて湿気が少なく、なるべく温度が一定の場所に設置してください。
動作温度：0 ℃～40 ℃
動作湿度：20 %～85 %
（ただし、結露なきこと）

隣接して使用しているラジオやテレビから2 m以上離してください。
また、同一コンセントでご使用の場合は、コンセントを別にしてください。
（ラジオやテレビに雑音が入ることがあります。）

CD-ROMに、テープ、シールやラベルなどを貼らないでください。
また、CD-ROMの裏面に、マジックやボールペンなどで文字を書かないでください。
（読み取り障害の原因になります。）

お手入れの際は、電源を切ってください。
（誤動作の原因になります。）

ジャック内部に触れないでください。
（故障の原因になります。）

ベンジンやシンナー、研磨剤などを使って本製品をふかないでください。
（本製品が変形・変色することがあります。）

固くしぼった柔らかい布でふいてください。
（台所用洗剤（中性）を水で薄め、柔らかい布に含ませ、固くしぼってふいてください。）

- 本製品を分解・改造することは法律で禁じられていますので、故障の際は、お買い上げの販売店に修理を依頼してください。
- 本製品は、外国為替および外国貿易法に定める規制対象貨物(または技術)に該当します。本製品を日本国外へ持ち出す場合は、同法に基づく輸出許可など必要な手続きをお取りください。
- 本製品は日本国内用です。国外での使用に対するサービスはいたしかねます。
- 本製品のデザイン、仕様は改善のため予告なしに変更することがあります。
- 本書は改善のため予告なしに変更することがあります。
- 本書の記載内容の一部、または全部を無断で転載することを禁じます。
- この装置は、情報処理装置等電波障害自主規制協議会(VCCI)の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
  取扱説明書に従って正しい取り扱いをしてください。
- 停電などの外部要因により生じたデータの損失ならびに、その他直接、間接の損害につきましては、当社は責任を負えない場合もございますので、あらかじめご了承ください。

正しくお使いいただくためのお願い

無線通信の使用範囲について

本製品と無線機器の距離が約50 cm〜約120 m (屋内見通し距離)・約50 cm〜約600 m (屋外見通し距離）の範囲でお使いください。ただし、IEEE 802.11aは5.2 GHz帯域の電波を使用しています。このため、IEEE 802.11aの屋外での使用は法律により禁止されています。
（無線機器の性能や周囲の環境によっては、使用範囲が狭くなります。）

本製品と無線機器の間に次のような物体があるときは設置場所を変更してください。
（電波を通しにくい物体が周囲にあると通信ができなかったり通信速度が遅くなる場合があります。）

- 鉄のドア
- スチール棚
- コンクリート、石、レンガなどの壁
- 防火ガラス

次のような機器と同時に本製品を使用しないでください。
（電波が混信したり、誤動作の原因になります。）

- 特定無線局や移動通信機器のある屋内
- 電子レンジの近く
- 盗難防止装置やPOSシステムなど2.4 GHz周波数帯域を利用している機器のある屋内

電波に関するご注意

本製品の使用周波数帯では、電子レンジなどの産業・科学・医療用機器のほか工場の製造ラインなどで使用されている移動体識別用の構内無線局（免許を要する無線局）および特定小電力無線局（免許を要しない無線局）ならびにアマチュア無線局（免許を要する無線局）が運用されています。

1. 本製品を使用する前に、近くで移動体識別用の構内無線局および特定小電力無線局ならびにアマチュア無線局が運用されていないことを確認してください。
2. 万一、本製品から移動体識別用の構内無線局に対して有害な電波干渉の事例が発生した場合には、速やかに使用周波数を変更するかまたは電波の発射を停止したうえ、お客様ご相談センター（☞ 182ページ）にご連絡いただき、混信回避のための処置などについてご相談してください。
3. その他、本製品から移動体識別用の特定小電力無線局あるいはアマチュア無線局に対して有害な電波干渉の事例が発生した場合など何かお困りのことが起きたときには、お客様ご相談センター（☞ 182ページ）へお問い合わせください。

オープンソースソフトウェアについて

本製品には、一部、Free Software FoundationのGPLおよびLGPLの条件やその他の条件に基づき提供されているオープンソースソフトウェアを使用しています。これらのソフトウェアにはそれぞれ該当する条件が適用されますので、ご使用にあたっては、GPL/LGPLについては付属のCD-ROMのopen_sourceフォルダの下のlicenseフォルダに格納されているgpl.txt、lgpl.txtを、その他のオープンソースソフトウェアについてはfreeware_headerフォルダに格納されているヘッダー集を、それぞれよくお読みください。なお、これらのソフトウェアにつきましては無保証とさせていただきますので、ご了承ください。

上記内容に関するお問い合わせ先: http://panasonic.co.jp/pcc/products/hnetwk/

お問い合わせフォームに必要事項を記入し、当社へご連絡ください。

セキュリティに関するご注意

本製品をご使用になる場合、下記のような被害を受けることが想定されますので、セキュリティ対策を十分に行ってください。

- 本製品を経由したお客様のプライバシー情報の漏えい
- 悪意の第三者による本製品の不正操作
- 悪意の第三者による本製品の妨害や停止

行うべきセキュリティ対策は下記のとおりです。

■ 不正な攻撃から守るため、最新のファームウェアを入手してバージョンアップする。（☞ 129ページ）(バージョンアップを怠ると、アクセスできなくなったり、情報の漏えいにつながることがあります。)

■ インターネットからのデータを直接受信する場合、コンピューターウィルスや不正プログラムの感染に対するチェックや駆除を行う。（☞ 95、101ページ）

■ 本製品へアクセスするためのユーザー名／パスワード、本製品に対する設定情報、アプリケーション設定情報、ログなどのシステム管理情報は、お客様の責任管理下にあります。それらの情報に関わる利用者または利用者グループ以外の第三者が、参照、更新、削除、複写できないようにアクセスを制限する。（☞ 128ページ）

■ 本製品を盗難に遭いにくい人目につかない場所に設置する。

■ お客様の利用情報(ビデオ映像・静止画・インターネットコンテンツなど)は、お客様の責任管理下にあります。それらの利用者情報に関わる利用者または利用者グループ以外の第三者が、参照、更新、削除、複写できないようにアクセスを制限する。（☞ 95ページ）

■ 以下のような場合は、必要に応じて個人情報をバックアップ（☞ 131ページ）したあと、本製品を初期化して工場出荷時設定に戻す。（☞ 132ページ）
  - 当社が関与できない外部業者に修理を依頼するとき。
  - 他人に譲渡するとき。

■ 本製品を廃棄するときは、本製品を初期化して工場出荷時設定に戻したり、あるいは、電気的消去や物理的破壊などの手段により本製品上の情報を抹消する。（☞ 132ページ）

パナソニック コミュニケーションズ株式会社

セキュリティに関するご注意

プライバシーに関するご注意

プライバシー・肖像権について

カメラの設置や利用につきましては、ご利用されるお客様の責任で被写体のプライバシー、肖像権などを考慮のうえ、行ってください。

※「プライバシーは、私生活をみだりに公開されないという法的保障ないし権利、もしくは自己に関する情報をコントロールする権利。また、肖像権は、みだりに他人から自らの容ぼう・姿態を撮影されたり、公開されない権利」と一般的に言われています。

セキュリティに関するご注意

無線LAN製品ご使用時におけるセキュリティに関するご注意！
お客様の権利（プライバシー保護）に関する重要な事項です

無線LANでは、イーサネットケーブルを使用するかわりに、電波を利用してパソコンなどと無線LANアクセスポイント間で情報のやり取りを行うため、電波の届く範囲であれば自由にネットワーク接続が可能であるという利点があります。
その反面、電波はある範囲内であれば障害物（壁など）を越えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

● 通信内容を盗み見られる

悪意ある第三者が、電波を故意に傍受し、
- ID、パスワード、通信画像やEメール

などの通信内容を盗み見られる可能性があります。

● 不正に侵入される

悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、
- 個人情報や機密情報を取り出す（情報漏えい）
- 特定の人物になりすまして通信し、不正な情報を流す（なりすまし）
- 傍受した通信内容を書き替えて発信する（改ざん）
- コンピュータウィルスなどを流しデータやシステムを破壊する（破壊）

などの行為をされてしまう可能性があります。

本来、無線LANアダプター、ホームネットワークカメラやカメラコントロールユニットをはじめとする無線LAN製品（以下、無線LAN製品という）は、これらの問題に対応するためのセキュリティに関する設定が用意されていますので、無線LAN製品のセキュリティに関する設定を行い使用することで、その問題が発生する可能性は少なくなります。

お客様がセキュリティ問題発生の可能性を少なくするためには、無線LAN製品をご使用になる前に、必ず無線LAN製品のセキュリティに関する設定を取扱説明書に従って行ってください。

なお、無線LANの仕様上、特殊な方法によりセキュリティに関する設定が破られることもありえますので、ご理解のうえ、ご使用ください。
セキュリティに関する設定について、お客様自身で対処できない場合には、お客様ご相談センター（☞ 保証とアフターサービス）までお問い合わせください。

当社では、お客様がセキュリティに関する設定を行わないで使用した場合の問題を十分理解したうえで、お客様自身の判断と責任においてセキュリティに関する設定を行い、無線LAN製品を使用することをおすすめします。
セキュリティに関する設定を行わない、あるいは、無線LANの仕様上やむをえない事情によりセキュリティの問題が発生してしまった場合、当社では、これによって生じた損害に対する責任を負いかねます。

上記文掲載URL: http://panasonic.co.jp/pcc/products/hnetwk/support/jeita_info.html

パナソニック コミュニケーションズ株式会社

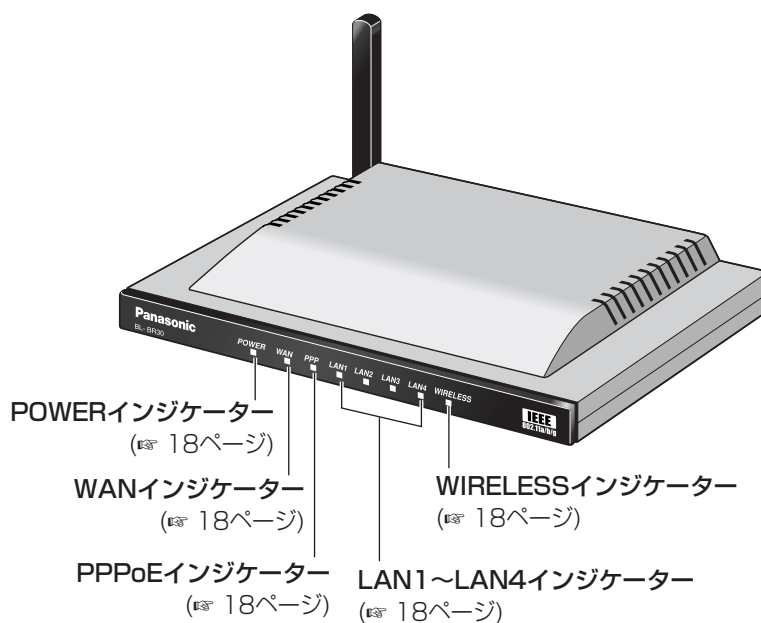
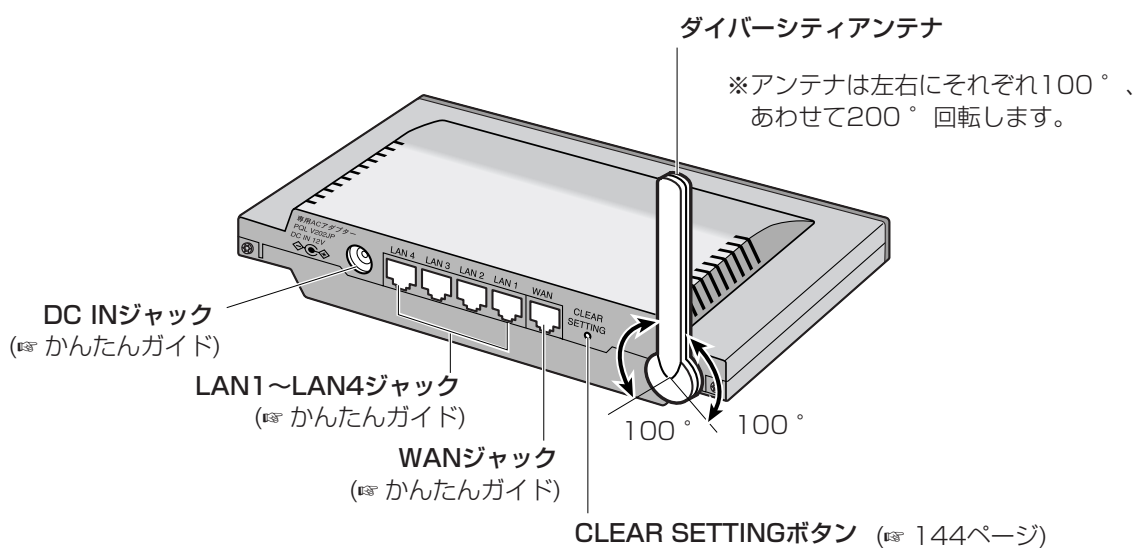
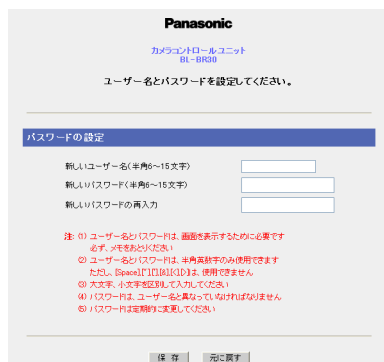
各部のなまえ

正　面

Panasonic
BL-BR30
POWER
WAN
PPP
LAN1
LAN2
LAN3
LAN4
WIRELESS
IEEE
802.11a/b/g
POWERインジケーター
(☞ 18ページ)
WANインジケーター
(☞ 18ページ)
PPPoEインジケーター
(☞ 18ページ)
WIRELESSインジケーター
(☞ 18ページ)
LAN1～LAN4インジケーター
(☞ 18ページ)

背　面

ダイバーシティアンテナ
※アンテナは左右にそれぞれ100°、
あわせて200°回転します。
LAN 4
LAN 3
LAN 2
LAN 1
WAN
CLEAR
SETTING
DC INジャック
(☞ かんたんガイド)
LAN1～LAN4ジャック
(☞ かんたんガイド)
WANジャック
(☞ かんたんガイド)
100°
100°
CLEAR SETTINGボタン (☞ 144ページ)

各部のなまえ

インジケーター

インジケーター	点灯色	表示内容
POWER	緑	電源が入っています。
	赤（点滅）	本製品に障害が発生しています。 コンセントからACコードのプラグを抜き、再度差し込んでください。
	緑 (点滅)	ファームウェアが壊れています。 ファームウェアファイルをダウンロードしてください。 (☞ 「ご使用の前に／困ったときには」の15ページ)
WAN	緑	モデム(またはONU)やイーサネットハブなどに接続されています。
	緑（点滅）	回線接続後、データ通信をしています。
LAN1～LAN4	緑	パソコン、イーサネットハブに接続されています。
	緑（点滅）	データ通信をしています。
WIRELESS	緑	無線機器と接続しています。
	緑（点滅）	無線でデータ通信しています。
	オレンジ	無線機器と接続されていません。
	消灯	通信モードが無効に設定されており、無線が使われていません。(☞ 69ページ)
PPPoE	緑（点滅）	PPPoE接続を試行中です。
	緑	PPPoE接続を完了しています。
	オレンジ	PPPoE認証エラーです。

トップページ

設定方法には、かんたん設定と詳細設定があります。トップページでいずれかの設定方法を選べます。
カメラモニター画面は、本製品に接続しているカメラ画像を表示します。

1 ウェブブラウザのアドレスバーに
http://blbr.webpage:8080を入力する
(ポート番号の工場出荷時設定は8080です。)

ユーザー名とパスワードの設定画面が表示されます。

2 **「新しいユーザー名」、「新しいパスワード」、「新しいパスワードの再入力」**を入力して、
保存 をクリックする

トップページが表示されます。

- 本製品の設定には、最低限、ユーザー名／パスワードによる認証を常に行ってください。
- 本製品へアクセスするためのユーザー名／パスワード、本製品に対する設定情報、アプリケーション設定情報、ログなどのシステム管理情報は、お客様の責任管理下にあります。それらの情報に関わる利用者または利用者グループ以外の第三者が、参照、更新、削除、複写できないようにアクセス制限をしたり、利用者以外にはユーザー名／パスワードやその他の設定・管理情報は秘密にしてください。

つづく

Panasonic

カメラコントロールユニット　BL-BR30

かんたん設定へ (☞ 21ページ)	かんたん設定	インターネット接続で必要最小限の設定を行います。
詳細設定へ (☞ 23ページ)	詳細設定	すべての項目について設定できます。
カメラモニター画面へ (☞ 26ページ)	カメラモニター画面	本製品に登録されているネットワークカメラの入口ページへ移動します。 ※カメラモニター画面をご使用の際は、必ずセキュリティ設定をご確認ください。 設定はこちら

- 工場出荷時設定では、ウェブブラウザのアドレスバーに**http://192.168.0.254:8080**と入力しても、トップページを表示させることができます。
- トップページから「かんたん設定」画面または「詳細設定」画面にアクセスするときには認証画面が表示されます(ウェブブラウザ起動後、初回のみ)。ユーザー名とパスワードを入力したあと OK を クリックしてログインしてください。
- 本製品のカメラモニター画面からカメラ画像を見るためには、本製品と対応ホームネットワークカメラ(別売品)との接続が完了している必要があります。詳しくは、カメラの取扱説明書を参照してください。

■ **トップページが表示されなかった場合**

- アドレスバーに**http://blbr.webpage:8080**を正しく入力しているか、確認してください。(ポート番号の工場出荷時設定は8080です。) 入力が正しいにもかかわらずトップページが表示されない場合には、**http://192.168.0.254:8080**を入力してください。
- 本製品に接続されているLANジャックに対応したLANインジケーターが点灯しているか確認してください。
- 本製品→パソコンの順番で電源を入れたか確認してください。
- トップページにアクセスするには、ウェブブラウザのプロキシサーバー設定が必要になる場合があります。(☞ 157ページ)

かんたん設定

インターネット接続の設定をします。

1 かんたん設定 をクリックする

2 接続形態を選んで、次へ をクリックする

接続形態メニューの中に該当する形態がないときは、「その他」を選んでください。

3 画面の指示に従って入力する

プロバイダーからの設定情報を参照してください。

4 設定を終えたら、保存 をクリックする

設定した内容が保存されます。

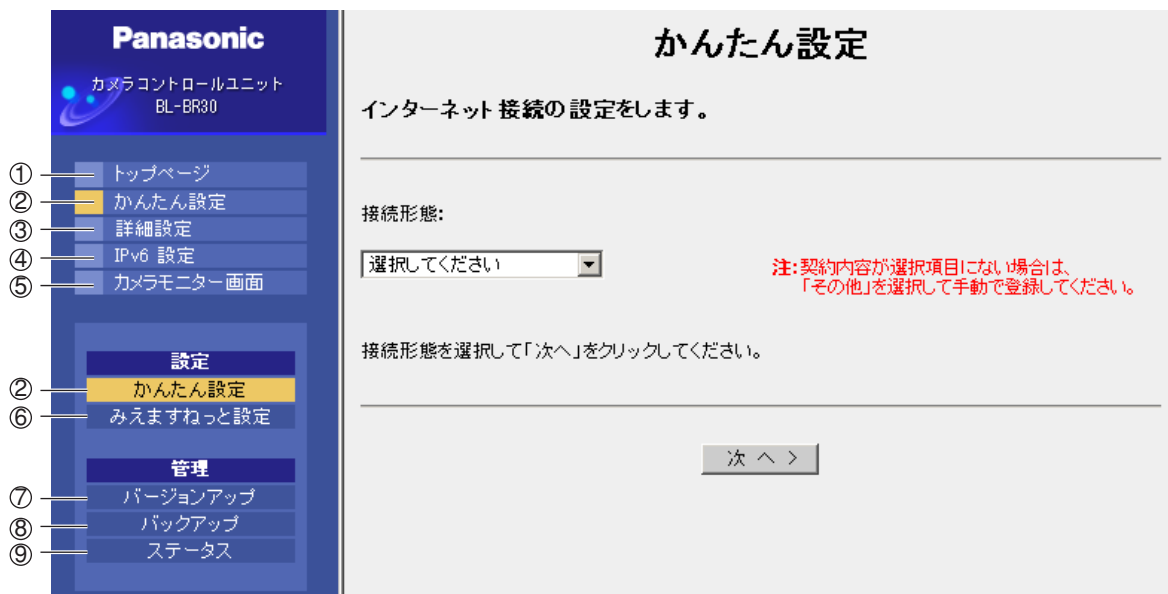
5 設定画面に、再起動 が表示されたら、それをクリックする

設定しました。

設定を完了するには再起動する必要があります。
後で再起動する場合は、再起動画面で再起動してください。
今すぐ再起動する場合は、再起動ボタンを押してください。

再起動

- 「かんたん設定」で登録したプロバイダーは、詳細設定画面にあるプロバイダー登録モニター中のNo. 1の欄に上書きされます。
- **「かんたん設定」に関する詳細な説明は、「かんたんガイド」を参照してください。**

つづく

① **トップページ：** トップページを表示します。
② **かんたん設定：** ウィザードに従って、インターネット接続の設定をします。
③ **詳細設定：** それぞれの設定画面を表示します。すべての項目について設定できます。
④ **IPv6設定：** IPv6ネットワークの設定を行います。
⑤ **カメラモニター画面：** 本製品に登録されているカメラ画像を見ることができます。

【設定】
② **かんたん設定：** インターネット接続の設定をします。
⑥ **みえますねっと設定：** みえますねっとの設定を行います。

【管理】
⑦ **バージョンアップ**※**：** ファームウェアを最新版に更新します。
⑧ **バックアップ：** 設定をバックアップファイルとして保存したり、バックアップファイルを使って設定を復元します。
⑨ **ステータス：** 回線接続状態などの情報を表示します。

※ パナソニックのサポートウェブサイトから最新のファームウェアファイルをダウンロードするには、インターネットに接続する必要があります。

詳細設定

パソコンからウェブブラウザを使ってIPv4でインターネットに接続するための設定を行うことができます。
メニュー画面で選んだ項目の内容がメイン画面に表示されます。
各項目ごとに操作に関するヘルプ画面を参照できます。

メニュー画面　　　　メイン画面

① **トップページ：** トップページを表示します。(☞ 19ページ)
② **かんたん設定：** ウィザードに従って、インターネット接続の設定をします。(☞ 21ページ)
③ **詳細設定：** それぞれの設定画面を表示します。すべての項目について設定できます。(☞ 本ページ)
④ **IPv6設定：** IPv6ネットワークの設定をします。(☞ 25ページ)
⑤ **カメラモニター画面：** 本製品に登録されているカメラ画像を見ることができます。(☞ 26ページ)

【設定】

⑥ **プロバイダー登録：** インターネットに接続するための基本的な設定をします。(☞ 31ページ)
⑦ **接続設定管理：** 接続するプロバイダーを設定します。また、PPPoEマルチセッションで接続する場合の詳細設定をします。(☞ 57ページ)
⑧ **カメラ設定：** カメラ自動登録機能の設定や、手動での追加登録・削除などを行います。(☞ 63ページ)
⑨ **無線設定：** 無線LANの動作モードや無線セキュリティの設定をします。(☞ 69ページ)
⑩ **みえますねっと設定：** みえますねっとの設定を行います。(☞ 79ページ)

つづく

機能を知る

【拡張機能】

⑪ **アドレス変換：** WAN(インターネット)側のグローバルアドレスとLAN側プライベートアドレスを相互変換して、インターネットの端末から本製品のネットワークにアクセスするための詳細な設定を行います。(☞ 81ページ)

⑫ **セキュリティ設定：** 本製品へのアクセス制限およびフィルタリングの設定をワンタッチで行い、自動的にログを保存します。(☞ 101ページ)

⑬ **オプション設定：** LAN(ホーム)側にアクセスするための設定と、インターネットに接続するための詳細な設定をします。(☞ 107ページ)

⑭ **VPN (PPTP) 設定：** ユーザー名とパスワードを設定することで、PPTP（Point-to-Point Tunneling Protocol）によるVPN（Virtual Private Network:私設仮想回線）を構築することができます。(☞ 120ページ)

【管理】

⑮ **パスワード設定：** 設定画面にアクセスするためのユーザー名やパスワードを変更します。(☞ 128ページ)

⑯ **バージョンアップ**※： ファームウェアを最新版に更新します。(☞ 129ページ)

⑰ **バックアップ**： 設定をバックアップファイルとして保存したり、バックアップファイルを使って設定を復元します。(☞ 131ページ)

⑱ **再起動：** 本製品を再起動します。(☞ 132ページ)

⑲ **初期化：** 本製品を初期化します。設定値が、工場出荷時の設定（☞ 165ページ）に戻ります。(☞ 132ページ)

⑳ **PPPoE接続／切断：** プロバイダーへのPPPoE接続を手動で開始または停止します。(☞ 133ページ)

㉑ **Ping：** IPアドレスをもった機器が接続されているか確認します。(☞ 135ページ)

【情報表示】

㉒ **ステータス：** 回線接続状態などの情報を表示します。(☞ 136ページ)

㉓ **ログ表示：** 「フィルタリングログ」、「UPnPログ(一般)」、「UPnPログ(CP機能)」、「接続／切断ログ」、「みえますねっとログ」、「VPN(PPTP)接続／切断ログ」、「メール送信ログ」を表示します。(☞ 139ページ)

㉔ **サポート：** 製品やサポートに関する情報を、インターネットから得ることができます。(☞ 143ページ)

㉕ **ヘルプ：** 設定画面のコマンドや機能について説明します。(☞ 143ページ)

※ パナソニックのサポートウェブサイトから最新のファームウェアファイルをダウンロードするには、インターネットへの接続が必要になります。

IPv6設定

パソコンからウェブブラウザを使ってIPv6でインターネットに接続するための設定を行うことができます。
メニュー画面で選んだ項目の内容がメイン画面に表示されます。
各項目ごとに操作に関するヘルプ画面を参照できます。

【設定】

① IPv6プロバイダー登録： IPv6でインターネットに接続するための基本的な設定をします。(☞ 44ページ)

【拡張機能】

② IPv6セキュリティ設定： 本製品へのアクセス制限およびフィルタリングの設定をワンタッチで行い、自動的にログを保存します。(☞ 101ページ)

③ IPv6オプション設定： IPv6でLAN(ホーム)側にアクセスするための設定と、インターネットに接続するための詳細な設定をします。(☞ 116ページ)

④ VPN（IPsec）設定： セキュリティポリシー・データベースを登録することで、IPsecによるVPN（Virtual Private Network:私設仮想回線）を構築することができます。(☞ 122ページ)

【管理】

⑤ VPN（IPsec）接続／切断: IPsec接続を手動で開始または停止します。(☞ 134ページ)

カメラモニター画面

本製品は、ウェブサーバー機能を内蔵しています。カメラモニター画面は、最大16台までのカメラ名と静止画像を一覧表示することができます。

■ LAN(ホーム)側からカメラ画像を見る

カメラモニター画面へアクセスし、カメラ画像を見ることができます。

1 ウェブブラウザを起動する

2 ウェブブラウザのアドレスバーに
http://blbr.webpage:ポート番号を入力する
ポート番号の工場出荷時設定は80です。ポート番号が80の場合は、ポート番号を入力する必要はありません。

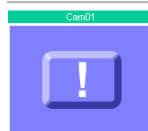
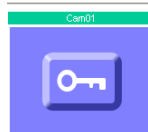
カメラモニター画面が表示されます。
表示されている画面をクリックすると、シングル動画を表示することができます。

- ！マークが表示された場合は、！マークをクリックするとカメラの初期パスワード画面が表示されます。カメラの設定画面に従って、設定してください。インターネット公開を「する」に設定すると、インターネット経由でカメラモニター画面上にカメラ画像を表示することができます。「しない」に設定すると、LAN側からアクセスしたときのみ、カメラモニター画面上でカメラ画像を見ることができます。
(工場出荷時設定状態のカメラを接続したときに表示されます。)

- 鍵マークが表示された場合は、鍵マークをクリックしてそのカメラのユーザー名とパスワードを入力してください。
(カメラに認証設定がされていると、鍵マークが表示されます。)

- カメラ画像の公開時間外では、青い無印の画面が表示されます。カメラ画像の公開中にもかかわらず、青い無印の画面が表示された場合は、 カメラ更新 をクリックしてください。
(認証設定確認中のカメラは、青い無印の画面が表示されることがあります。)

- 本製品とカメラの通信で切断が発生した場合、鍵マーク(カメラに認証設定がされている場合)、あるいは青い無印の画面が表示されることがあります。この場合は本製品とカメラの接続、カメラの電源などを確認してから、 カメラ更新 をクリックしてください。

つづく

3 アクセスしたいカメラ枠をクリックする

認証画面が表示された場合は、カメラのユーザー名とパスワードを入力してください。カメラ画像が表示されます。

- カメラモニター画面を更新するときは、設定画面上の カメラ更新 をクリックしてください。ウェブブラウザの更新ボタンをクリックすると、カメラ画像が鍵マークに戻ります。
- 一度カメラのユーザー名とパスワードを入力しカメラ画像を表示させたあとは、カメラモニター画面には鍵マークではなく、カメラ画像が表示されます。詳細設定など他の画面を表示させると鍵マークに戻りますが、再度鍵マークをクリックすると認証画面が表示されることなくカメラ画像が表示されます。
- 松下電器産業(株)製の「Tナビ」対応テレビ／チューナーのウェブブラウザ機能を使った場合、カメラ画像は表示されず鍵マークのままです。

プライバシー・肖像権について

カメラの設置や利用につきましては、ご利用されるお客様の責任で被写体のプライバシー、肖像権などを考慮のうえ、行ってください。

※「プライバシーは、私生活をみだりに公開されないという法的保障ないし権利、もしくは自己に関する情報をコントロールする権利。また、肖像権は、みだりに他人から自らの容ぼう・姿態を撮影されたり、公開されない権利」と一般的に言われています。

■ カメラモニター画面上にカメラ画像が表示されなかった場合

- WANインジケーター、および本製品に接続されているLANジャックに対応したLANインジケーターが点灯しているか確認してください。
- カメラモニター画面にアクセスするには、ウェブブラウザのプロキシサーバー設定が必要になる場合があります。(☞ 157ページ)
- モデム(またはONU)→本製品→パソコンの順で電源を入れたか確認してください。
- カメラモニター画面にカメラ名、 × マーク、青い無印の画面もしくは白画面が表示されているときは、 カメラ更新 をクリックしてください。
- カメラモニター画面に！マークが表示されているときは、！マークをダブルクリックしてください。カメラの初期パスワード画面が表示されます。

■ WAN(インターネット)側からカメラ画像を見る

WAN側からカメラモニター画面へアクセスし、カメラ画像を見ることができます。

WAN(インターネット)側からカメラ画像を見るためには、本製品がWAN(インターネット)に接続されている必要があります。インターネットへの接続方法については、かんたんガイドまたは「機能を使う」(☞ 31ページ)以降を参照してください。

1 ウェブブラウザを起動する

2 ウェブブラウザのアドレスバーに
http://WAN側のIPアドレスまたはURL: ポート番号を入力する
例：http://10.75.68.251:80/
　　http://www.example.com:80/
ポート番号の工場出荷時設定は80です。ポート番号が80の場合は、ポート番号を入力する必要はありません。

- WAN側IPアドレスは設定画面のステータスで確認することができます。(☞ 136ページ)
- 本製品を固定IPサービスでないサービスで使用する場合は、IPアドレスが随時変更されますので、みえますねっとサービスのご利用をおすすめします。(☞ 79ページ)

3 Enter を押す
カメラモニター画面が表示されます。

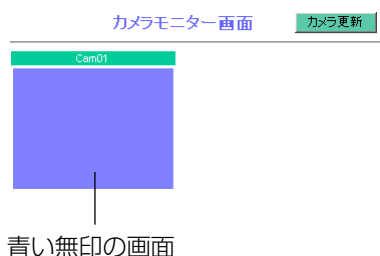
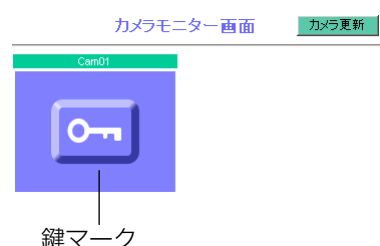
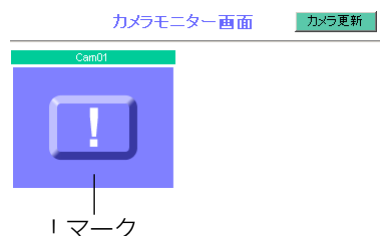
カメラモニター画面　カメラ更新

- ！マークが表示された場合は、！マークをクリックするとカメラの初期パスワード画面が表示されます。カメラの設定画面に従って、設定してください。インターネット公開を「する」に設定すると、インターネット経由でカメラモニター画面上にカメラ画像を表示することができます。「しない」に設定すると、LAN側からアクセスしたときのみ、カメラモニター画面上でカメラ画像を見ることができます。
  (工場出荷時設定状態のカメラを接続したときに表示されます。)

- 鍵マークが表示された場合は、鍵マークをクリックしてそのカメラのユーザー名とパスワードを入力してください。
  (カメラに認証設定がされていると、鍵マークが表示されます。)

- カメラ画像の公開時間外では、青い無印の画面が表示されます。カメラ画像の公開中にもかかわらず、青い無印の画面が表示された場合は、 カメラ更新 をクリックしてください。
  (認証設定確認中のカメラは、青い無印の画面が表示されることがあります。)

- 本製品とカメラの通信で切断が発生した場合、鍵マーク(カメラに認証設定がされている場合)、あるいは青い無印の画面が表示されることがあります。この場合は本製品とカメラの接続、カメラの電源などを確認してから、 カメラ更新 をクリックしてください。

つづく

4 アクセスしたいカメラ枠をクリックする

認証画面が表示された場合は、カメラのユーザー名とパスワードを入力してください。カメラ画像が表示されます。

■ **カメラモニター画面が表示されなかった場合**

- アドレスバーに**http://WAN側IPアドレスまたはURL: ポート番号**が正しく入力されているか、確認してください。
- ウェブサイトにアクセスするには、ウェブブラウザのプロキシサーバー設定が必要になる場合があります。（☞ 157ページ）
- カメラモニター画面にカメラ名と ✕ マークもしくは白画面が表示されているときは、カメラ更新 をクリックしてください。

- お客様の利用情報(ビデオ映像・静止画・インターネットコンテンツなど)は、お客様の責任管理下にあります。それら利用者情報に関わる利用者または利用者グループ以外の第三者が、参照、更新、削除、複写できないようにアクセス制限をしてください。
- カメラモニター画面やカメラの設定を変更する場合は、「カメラを使う」(☞ 63ページ) を参照してください。

プライバシー・肖像権について

カメラの設置や利用につきましては、ご利用されるお客様の責任で被写体のプライバシー、肖像権などを考慮のうえ、行ってください。

※「プライバシーは、私生活をみだりに公開されないという法的保障ないし権利、もしくは自己に関する情報をコントロールする権利。また、肖像権は、みだりに他人から自らの容ぼう・姿態を撮影されたり、公開されない権利」と一般的に言われています。

IPv4接続のプロバイダーを登録する

プロバイダー登録画面では、本製品と接続するプロバイダーを新規登録 (☞ 32ページ) したり、編集、削除 (☞ 55ページ) することができます。インターネットへの接続方法はプロバイダーによって異なります。プロバイダーからの設定情報を見て、接続方法を選んでください。

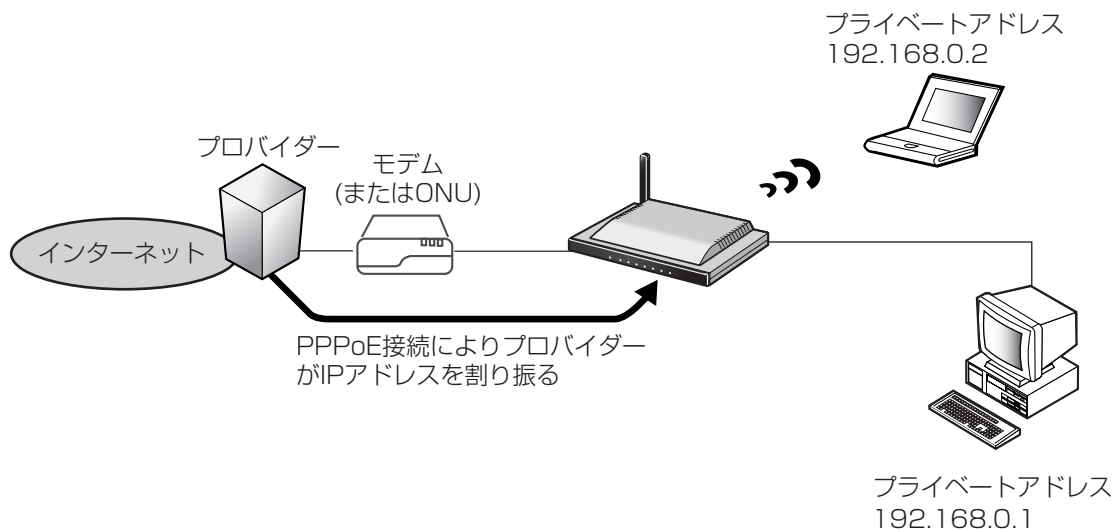
インターネットの接続方法 がどれに該当するかなど、サービス内容や契約内容についての詳細はご契約のプロバイダーにお問い合わせください。

データ入力欄 (次ページ以降の入力について)

接続方法	説　明
DHCP接続 (☞ 35ページ) ● プロバイダーの名称 ● デバイス名 ● ゲートウェイ ● DNSサーバー1／DNSサーバー2 ● ドメイン名	プロバイダーがDHCPサーバー機能を利用している場合、基本的に設定値の入力は必要ありませんが、デバイス名、ゲートウェイ、DNSサーバー1、DNSサーバー2、ドメイン名の入力を求められる場合があります。プロバイダーからの設定情報を参照のうえ、必要に応じて入力してください。
端末型Static接続 (☞ 37ページ) LAN型Static接続 (☞ 42ページ) ● プロバイダーの名称 ● IPアドレス ● サブネットマスク ● ゲートウェイ ● DNSサーバー1／DNSサーバー2 ● ドメイン名	プロバイダーが指定したIPアドレス、サブネットマスク、ゲートウェイ、DNSサーバー1、DNSサーバー2を入力してください。 プロバイダーから指定がある場合は、ドメイン名を入力してください。
端末型PPPoE接続 (☞ 32ページ) LAN型PPPoE接続 (☞ 39ページ) ● プロバイダーの名称 ● ユーザー名／パスワード ● サービス名 ● アクセスコンセントレーター名 ● DNSサーバー1／DNSサーバー2 ● ドメイン名 ● 本製品のIPアドレス／ 　サブネットマスク (LAN型接続のみ)	PPPoE接続をする場合、これらに関するデータの入力が必要になります。 プロバイダーからの設定情報を参照のうえ、ユーザー名とパスワードを入力してください。 プロバイダーから指定がある場合は、サービス名、アクセスコンセントレーター名、DNSサーバー1、DNSサーバー2、ドメイン名を入力してください。

※ データ入力欄に設定する内容がない場合は、空欄のままにしてください。

■ 端末型PPPoE接続の場合

端末型PPPoE接続の設定は、次の手順に従ってください。

1 プロバイダー登録 を選ぶ

2 プロバイダー登録モニター中で 登録／編集 をクリックする

3 端末型の **「PPPoE接続」** を選ぶ

つづく

4 **「プロバイダーの名称」**を入力する

半角20文字 (全角10文字) 以内で入力してください。
右の例では、「abcde」を入力しています。

5 **「ユーザー名」、「パスワード」**を入力し、プロバイダーから指定がある場合は**「サービス名」、「アクセスコンセントレーター名」、「DNSサーバー1、2」、「ドメイン名」**を入力する

プロバイダーからの設定情報を参照してください。
元の設定に戻すには、 元に戻す をクリックしてください。

6 設定を終えたら、 **保存して接続設定管理へ** をクリックする

接続設定管理画面が表示されます。

7 プロバイダー設定のメインセッションで、ステップ4で入力したプロバイダーを選ぶ

マルチセッション機能を使用する場合は、サブセッションの設定をします。「PPPoEマルチセッション機能」(☞ 59ページ) を参照してください。

8 設定を終えたら、 **保存** をクリックする

設定した内容が保存されます。

保存中は絶対に電源を切らないでください。保存中に電源を切ると本製品が正常に動作しなくなる可能性があります。

つづく

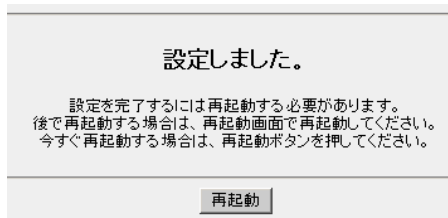
9 設定画面に 再起動 が表示されたら、それをクリックする

10 パソコンを再起動する

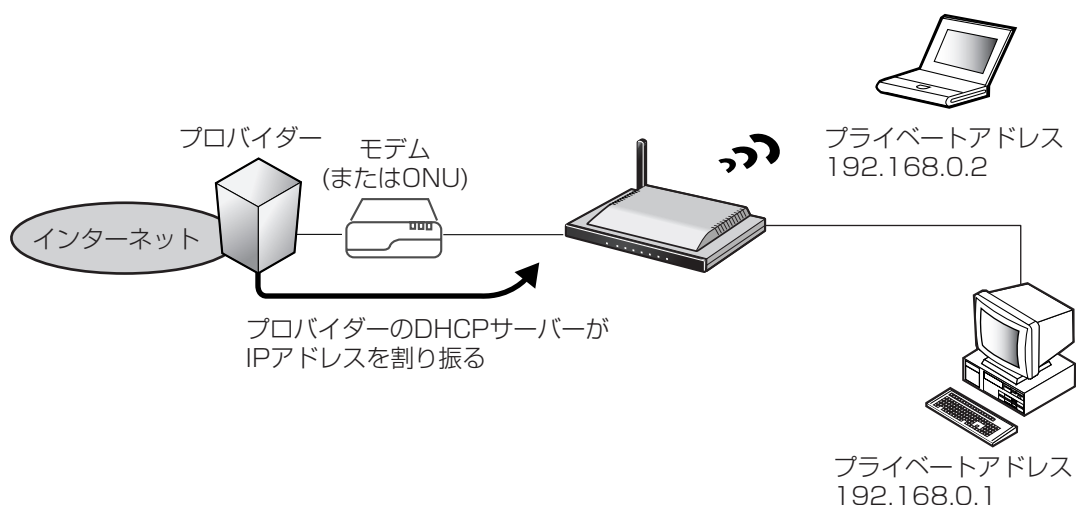
インターネットへの接続を確認してください。
(☞ 56ページ)

設定しました。

設定を完了するには再起動する必要があります。
後で再起動する場合は、再起動画面で再起動してください。
今すぐ再起動する場合は、再起動ボタンを押してください。

再起動

- 登録／編集を行った場合、LAN(ホーム)側に接続しているすべてのパソコンを再起動してください。
- 設定完了後パソコンを増設する場合は、増設するパソコンをLAN1～LAN4ジャックに接続してから再起動してください。
- 利用するプロバイダーから指示がある場合、MTU値を変更してください。指示がない場合は工場出荷時設定(1492)のままにしてください。(☞ 111ページ)

■ DHCP接続(DHCPサーバーを使ったインターネット接続)の場合

DHCP接続(プロバイダーからIPアドレスが自動的に割り振られる)は、次の手順に従ってください。

1 [プロバイダー登録] を選ぶ

2 プロバイダー登録モニター中で [登録／編集] をクリックする

3 「DHCP接続」を選ぶ

接続モード登録　現在の設定

--- 端末型 ---

PPPoE接続

DHCP接続

Static接続

--- LAN型 ---

PPPoE接続

Static接続

4 **「プロバイダーの名称」**を入力する

半角20文字 (全角10文字) 以内で入力してください。右の例では、「abcde」を入力しています。

5 プロバイダーから指定がある場合は **「デバイス名」**※、**「ゲートウェイ」**、**「DNSサーバー1、2」**、**「ドメイン名」**を入力する

プロバイダーからの設定情報を参照してください。元の設定に戻すには、[元に戻す] をクリックしてください。

※「デバイス名」は、プロバイダーによってはパソコンのコンピューター名入力欄に入力するIDと指示されている場合があります。

6 設定を終えたら、[保存して接続設定管理へ] をクリックする

接続設定管理画面が表示されます。

7 プロバイダー設定のプロバイダー選択の中から、ステップ4で入力したプロバイダーを選ぶ

8 設定を終えたら、[保存] をクリックする

設定した内容が保存されます。

保存中は絶対に電源を切らないでください。保存中に電源を切ると本製品が正常に動作しなくなる可能性があります。

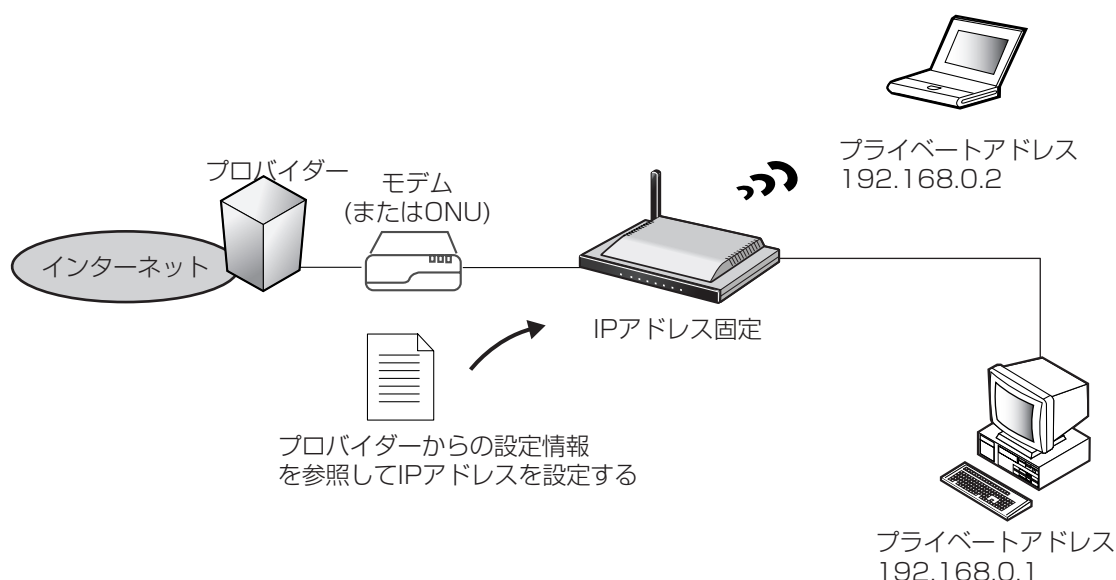
9 設定画面に [再起動] が表示されたら、それをクリックする

10 パソコンを再起動する

インターネットへの接続を確認してください。
(☞ 56ページ)

- 登録／編集を行った場合、LAN(ホーム)側に接続しているすべてのパソコンを再起動してください。
- 設定完了後パソコンを増設する場合は、増設するパソコンをLAN1～LAN4ジャックに接続してから再起動してください。

■ 端末型Static接続(1つの固定IPアドレスによるインターネット接続)の場合

プロバイダーからの設定情報にIPアドレスやゲートウェイアドレスなどの値を入力するように指示がある場合は、本製品にこれらの値を入力する必要があります。

1 プロバイダー登録 を選ぶ

2 プロバイダー登録モニター中で 登録／編集 をクリックする

3 端末型の「**Static接続**」を選ぶ

つづく

4 「プロバイダーの名称」を入力する

半角20文字 (全角10文字) 以内で入力してください。右の例では、「abcde」を入力しています。

5 「IPアドレス」、「サブネットマスク」、「ゲートウェイ」、「DNSサーバー1、2」を入力し、プロバイダーから指定がある場合は「ドメイン名」を入力する

プロバイダーからの設定情報を参照してください。元の設定に戻すには、 取り消し をクリックしてください。

6 設定を終えたら、 保存して接続設定管理へ をクリックする

接続設定管理画面が表示されます。

7 プロバイダー設定のプロバイダーメニューの中から、ステップ4で入力したプロバイダーを選ぶ

8 設定を終えたら、 保存 をクリックする

設定した内容が保存されます。

保存中は絶対に電源を切らないでください。保存中に電源を切ると本製品が正常に動作しなくなる可能性があります。

9 設定画面に 再起動 が表示されたら、それをクリックする

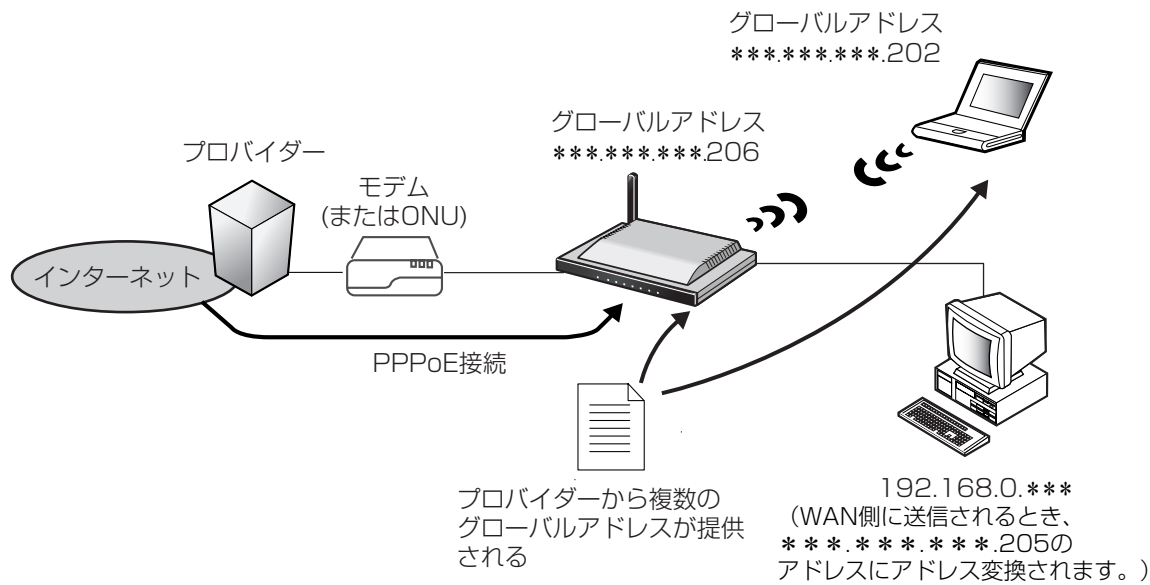
10 パソコンを再起動する

インターネットへの接続を確認してください。
(☞ 56ページ)

- 登録／編集を行った場合、LAN(ホーム)側に接続しているすべてのパソコンを再起動してください。
- 設定完了後パソコンを増設する場合は、増設するパソコンをLAN1～LAN4ジャックに接続してから再起動してください。

■ LAN型PPPoE接続の場合

LAN型PPPoE接続は、複数のグローバルアドレスをプロバイダーから提供される接続形態です。

LAN型PPPoE接続の設定は、次ページの手順に従ってください。

本ページは、プロバイダーへの接続を説明しています。LAN型PPPoEで実際にグローバルアドレスを使用する場合は94ページを参照してください。

＊＊＊.＊＊＊.＊＊＊.200/29というネットワークアドレスとプレフィックスをプロバイダーから提供された場合、グローバルアドレスの使いかたは次表のようになります。LAN型PPPoE接続またはLAN型Static接続をご使用になる場合に参照ください。

<LAN型接続の場合の配布例>

設定項目	LAN型PPPoE接続	LAN型Static接続
ネットワークアドレス	＊＊＊.＊＊＊.＊＊＊.200	
本製品のグローバルアドレス	＊＊＊.＊＊＊.＊＊＊.206	
本製品のゲートウェイ	–	＊＊＊.＊＊＊.＊＊＊.201 (プロバイダーから指定されたゲートウェイアドレス)
	＊＊＊.＊＊＊.＊＊＊.201– ＊＊＊.＊＊＊.＊＊＊.204	＊＊＊.＊＊＊.＊＊＊.202– ＊＊＊.＊＊＊.＊＊＊.204
カメラまたはパソコンに設定するのゲートウェイ	＊＊＊.＊＊＊.＊＊＊.206(本製品のグローバルアドレスを設定)	
本製品のLAN型IPマスカレード(アドレス変換)	＊＊＊.＊＊＊.＊＊＊.205 LANに接続するカメラやパソコンの台数に対してグローバルアドレスが不足している場合、IPマスカレード機能を使って指定されたグローバルアドレスで接続する	
ブロードキャストアドレス	＊＊＊.＊＊＊.＊＊＊.207	

つづく

1 プロバイダー登録 を選ぶ

2 プロバイダー登録モニター中で 登録／編集 をクリックする

3 LAN型の**「PPPoE接続」**を選ぶ

4 **「プロバイダーの名称」**を入力する

半角20文字（全角10文字）以内で入力してください。
右の例では、「abcde」を入力しています。

5 **「ユーザー名」、「パスワード」、「DNSサーバー1、2」**を入力し、プロバイダーから指定がある場合は**「サービス名」、「アクセスコンセントレーター名」、「ドメイン名」**を入力する

プロバイダーからの設定情報を参照してください。

本製品のIPアドレスについて
プロバイダーから割り振られたグローバルアドレスの１つとサブネットマスクを「本製品のIPアドレス」に入力してください。本製品からインターネットに直接送信するときに、このIPアドレスを送信元IPアドレスとして使います。

元の設定に戻すには、 元に戻す をクリックしてください。

プロバイダーの名称
プロバイダーの名称 abcde
プロバイダー登録
ユーザー名
パスワード
プロバイダーから指定があるときに入力
サービス名
アクセスコンセントレーター名
DNSサーバー1
DNSサーバー2
ドメイン名
本製品のIPアドレス
IPアドレス
サブネットマスク
注：WAN(インターネット)側のIPアドレスであり、
本製品からWAN(インターネット)側に直接送信するときに
使用されます。(例：本製品からのPing)
静的アドレス変換およびIPマスカレードで使用するIPアドレスは、
アドレス変換の“LAN型”で設定してください。
保存して接続設定管理へ　元に戻す　戻る

つづく

6 設定を終えたら、［保存して接続設定管理へ］をクリックする

接続設定管理画面が表示されます。

7 プロバイダー設定のメインセッションで、ステップ4で入力したプロバイダーを選ぶ

マルチセッション機能を使用する場合は、サブセッションの設定をします。「PPPoEマルチセッション機能」（☞ 59ページ）を参照してください。

8 設定を終えたら、［保存］をクリックする

設定した内容が保存されます。

保存中は絶対に電源を切らないでください。保存中に電源を切ると本製品が正常に動作しなくなる可能性があります。

9 設定画面に［再起動］が表示されたら、それをクリックする

設定しました。

設定を完了するには再起動する必要があります。
後で再起動する場合は、再起動画面で再起動してください。
今すぐ再起動する場合は、再起動ボタンを押してください。

［再起動］

10 パソコンにグローバルアドレスを割り振る

- **パソコンにグローバルアドレスを固定する**
  160ページの「パソコンのIPアドレスを固定するには」を参照してください。
- **パソコンにプライベートアドレスを固定し、静的NATを利用してグローバルアドレスを設定する**
  160ページの「パソコンのIPアドレスを固定するには」、および88ページの「静的NAT」を参照してください。

11 パソコンを再起動する

インターネットへの接続を確認してください。
（☞ 56ページ）

- 登録／編集を行った場合、LAN(ホーム)側に接続しているすべてのパソコンを再起動してください。
- 設定完了後パソコンを増設する場合は、増設するパソコンをLAN1～LAN4ジャックに接続してから再起動してください。

■ LAN型Static接続(複数の固定IPアドレスによるインターネット接続)の場合

プロバイダーからの設定情報にIPアドレスやゲートウェイアドレスなどの値を入力するように指示がある場合は、本製品にこれらの値を入力する必要があります。

＊＊＊.＊＊＊.＊＊＊.200/29というネットワークアドレスとプレフィックスを提供された場合のグローバルアドレスの使いかたについては、39ページの<**LAN型接続の場合の配布例**>表を参照ください。

1 **プロバイダー登録** を選ぶ

2 プロバイダー登録モニター中で **登録／編集** をクリックする

3 LAN型の**「Static接続」**を選ぶ

つづく

4 「プロバイダーの名称」を入力する

半角20文字（全角10文字）以内で入力してください。
右の例では、「abcde」を入力しています。

5 「IPアドレス」、「サブネットマスク」、「ゲートウェイ」、「DNSサーバー1、2」を入力し、プロバイダーから指定がある場合は「ドメイン名」を入力する

プロバイダーからの設定情報を参照してください。
元の設定に戻すには、［取り消し］をクリックしてください。

6 設定を終えたら、［保存して接続設定管理へ］をクリックする

接続設定管理画面が表示されます。

7 プロバイダー設定のプロバイダーメニューの中から、ステップ4で入力したプロバイダーを選ぶ

8 設定を終えたら、［保存］をクリックする

設定した内容が保存されます。

保存中は絶対に電源を切らないでください。保存中に電源を切ると本製品が正常に動作しなくなる可能性があります。

9 設定画面に［再起動］が表示されたら、それをクリックする

10 パソコンを再起動する

インターネットへの接続を確認してください。
（☞ 56ページ）

- 登録／編集を行った場合、LAN(ホーム)側に接続しているすべてのパソコンを再起動してください。
- 設定完了後パソコンを増設する場合は、増設するパソコンをLAN1～LAN4ジャックに接続してから再起動してください。

本ページは、プロバイダーへの接続を説明しています。LAN型PPPoEで実際にグローバルアドレスを使用する場合は94ページを参照してください。

IPv6接続のプロバイダーを登録する

メニューから「IPv6設定」を選んだときのみ、表示される項目です。IPv6プロバイダー登録画面では、本製品と接続するIPv6対応プロバイダーを新規登録したり、編集したり、削除することができます。IPv6ネットワークへの接続方法はプロバイダーによって異なります。プロバイダーからの情報を見て、接続方法を選んでください。

プロバイダー登録モニター

No.	プロバイダー名称	接続モード	登録編集	登録削除
1	abcde	6to4	登録/編集	削除
2			登録/編集	削除
3			登録/編集	削除
4			登録/編集	削除

IPv6ネットワークへの接続方法 がどれに該当するかなど、サービス内容や契約内容についての詳細はご契約のプロバイダーにお問い合わせください。

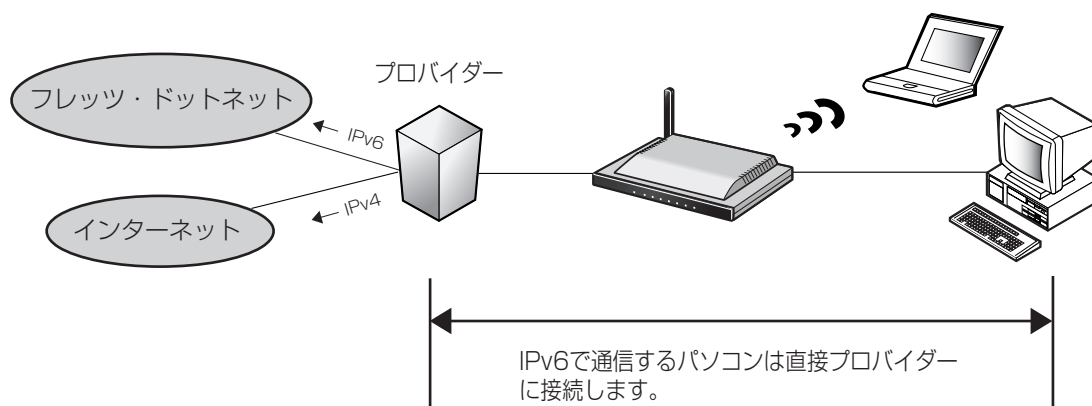
接続確認済みのIPv6サービス対応プロバイダーについては、パナソニックのサポートウェブサイト（http://panasonic.co.jp/pcc/products/hnetwk/support/）を参照してください。

データ入力欄（次ページ以降の入力について）

接続方法	説　明
IPv6ブリッジ接続（☞45ページ） ● プロバイダーの名称	フレッツ・ドットネットを利用しているときに、選択してください。特に設定項目はありません。
トンネル接続（☞47ページ） ● プロバイダーの名称 ● 接続先IPアドレス ● LAN側プレフィックス ● IPv6 DNSサーバー1／ IPv6 DNSサーバー2 ● WAN側IPv6アドレス	プロバイダーが指定した、接続先IPアドレス、LAN側プレフィックスを入力してください。プロバイダーから指定がある場合は、IPv6 DNSサーバー1、IPv6 DNSサーバー2、WAN側IPv6アドレスを入力してください。
6to4接続（☞49ページ） ● プロバイダーの名称 ● 接続先IPアドレス	6to4接続は、IPv4とIPv6の相互接続性を検証するために実験的に公開されている接続方式です。ウェブサイト（http://www.6to4.jp/）を参考にして設定してください。
PPPoE IPv4/IPv6接続（☞51ページ） ● プロバイダーの名称 ● IPv6 DNSサーバー1／ IPv6 DNSサーバー2	プロバイダーから指定がある場合は、IPv6 DNSサーバー1、IPv6 DNSサーバー2を入力してください。
Static V6接続（☞53ページ） ● プロバイダーの名称 ● WAN側IPv6アドレス ● LAN側プレフィックス ● IPv6デフォルトゲートウェイ ● IPv6 DNSサーバー1／ IPv6 DNSサーバー2 ● ドメイン名	プロバイダーから指定された、WAN側IPv6アドレス、LAN側プレフィックス、IPv6デフォルトゲートウェイ、IPv6 DNSサーバー1、IPv6 DNSサーバー2を入力してください。 プロバイダーから指定がある場合は、ドメイン名を入れてください。

※ データ入力欄に設定する内容がない場合は、空欄のままにしてください。

■ IPv6ブリッジ接続の場合

本製品はIPv6パケットに対してハブとして動作します。
IPv6ブリッジ接続の設定は、次の手順に従ってください。

1 [IPv6プロバイダー登録] を選ぶ

2 IPv6プロバイダー登録モニター中で [登録／編集] をクリックする

3 「IPv6ブリッジ接続」を選ぶ

接続モード登録　現在の設定

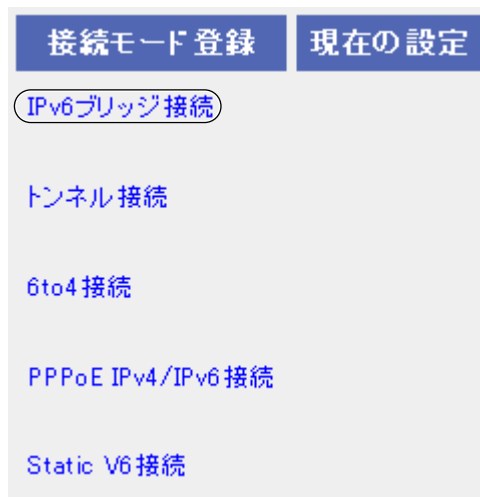
IPv6ブリッジ接続

トンネル接続

6to4接続

PPPoE IPv4/IPv6接続

Static V6接続

つづく

4 「プロバイダーの名称」を入力する

半角20文字（全角10文字）以内で入力してください。
右の例では、「abcde」を入力しています。

5 設定を終えたら、［保存して接続設定管理へ］をクリックする

接続設定管理画面が表示されます。

6 プロバイダー設定のプロバイダー選択の中から、ステップ4で入力したプロバイダーを選ぶ

7 設定を終えたら、［保存］をクリックする

設定した内容が保存されます。

保存中は絶対に電源を切らないでください。保存中に電源を切ると本製品が正常に動作しなくなる可能性があります。

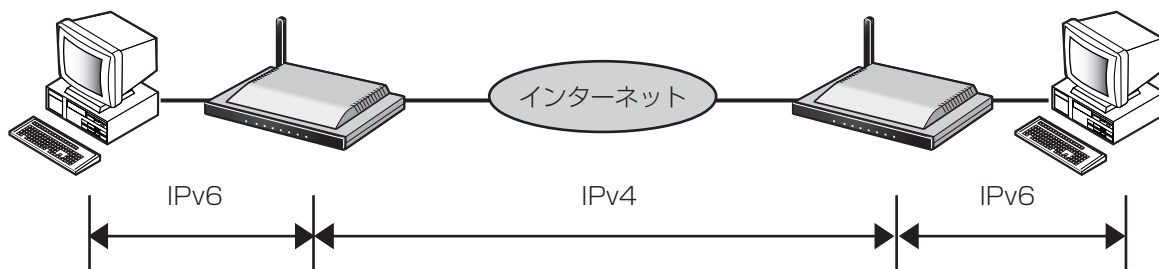
8 設定画面に［再起動］が表示されたら、それをクリックする

9 パソコンを再起動する

インターネットへの接続を確認してください。
（☞ 56ページ）

- IPv6ブリッジ接続のときは、本製品のIPv6に関するセキュリティなどの設定は、機能しません。
- 登録／編集を行った場合、LAN(ホーム)側に接続しているすべてのパソコンを再起動してください。
- 設定完了後パソコンを増設する場合は、増設するパソコンをLAN1～LAN4ジャックに接続してから再起動してください。

■ トンネル接続の場合

IPv6パケットをIPv4パケットでカプセル化して、IPv4ネットワークでIPv6通信を行うことができます。
トンネル接続は、次の手順に従ってください。

1 IPv6プロバイダー登録 を選ぶ

2 IPv6プロバイダー登録モニター中で 登録／編集 をクリックする

3 **「トンネル接続」**を選ぶ

4 **「プロバイダーの名称」**を入力する

半角20文字 (全角10文字) 以内で入力してください。
右の例では、「abcde」を入力しています。

5 **「接続先IPアドレス」、「LAN側プレフィックス」**を入力し、プロバイダーから指定がある場合は、**「IPv6 DNSサーバー1」、「IPv6 DNSサーバー2」、「WAN側IPv6アドレス」**を入力する

プロバイダーからの設定情報を参照してください。
元の設定に戻すには、 元に戻す をクリックしてください。

プロバイダー名称
プロバイダー名称
接続先設定
接続先IPアドレス
LAN側プレフィックス
プレフィックス /
プロバイダーから指定があるときに入力
IPv6 DNSサーバ1
IPv6 DNSサーバ2
WAN側IPv6アドレス /
保存して接続設定管理へ　元に戻す　戻る

つづく

6 設定を終えたら、 保存して接続設定管理へ をクリックする

接続設定管理画面が表示されます。

7 プロバイダー設定のプロバイダー選択の中から、ステップ4で入力したプロバイダーを選ぶ

8 設定を終えたら、 保存 をクリックする

設定した内容が保存されます。

保存中は絶対に電源を切らないでください。保存中に電源を切ると本製品が正常に動作しなくなる可能性があります。

9 設定画面に 再起動 が表示されたら、それをクリックする

10 パソコンを再起動する

インターネットへの接続を確認してください。
(☞ 56ページ)

- 登録／編集を行った場合、LAN(ホーム)側に接続しているすべてのパソコンを再起動してください。
- 設定完了後パソコンを増設する場合は、増設するパソコンをLAN1～LAN4ジャックに接続してから再起動してください。
- IPv4のプロバイダー設定を必ず行ってください。

■ 6to4接続の場合

6to4接続は、トンネル接続の一種で、実験サービスとして利用することができます。6to4接続をするためにIPv6対応プロバイダーと契約する必要はありません。
6to4接続は、以下の手順で設定してください。

1 IPv6プロバイダー登録 を選ぶ

2 IPv6プロバイダー登録モニター中で
登録／編集 をクリックする

3 「6to4接続」を選ぶ

4 「プロバイダーの名称」を入力する

半角20文字（全角10文字）以内で入力してください。
右の例では、「abcde」を入力しています。

5 6to4接続する相手先のルーターのIPv4アドレスを入力する

元の設定に戻すには、 取り消し をクリックしてください。

接続先IPアドレスは、公開されている6to4リレールーターのIPアドレスを設定してください。6to4リレールーターは公開されており、インターネット上で検索することができます。

6 設定を終えたら、 保存して接続設定管理へ をクリックする

接続設定管理画面が表示されます。

つづく

7 プロバイダー設定のプロバイダー選択の中から、ステップ4で入力したプロバイダーを選ぶ

8 設定を終えたら、［保存］をクリックする

設定した内容が保存されます。

- **保存中は絶対に電源を切らないでください。保存中に電源を切ると本製品が正常に動作しなくなる可能性があります。**
- IPv4のプロバイダー設定を必ず行ってください。

9 設定画面に［再起動］が表示されたら、それをクリックする

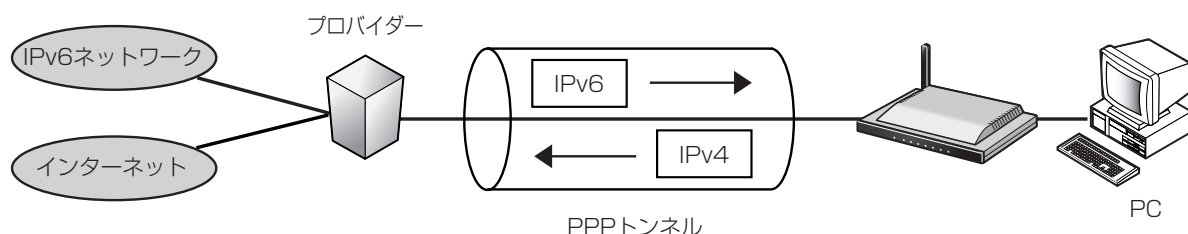
10 パソコンを再起動する

インターネットへの接続を確認してください。
(☞ 56ページ)

- 登録／編集を行った場合、LAN(ホーム)側に接続しているすべてのパソコンを再起動してください。
- 設定完了後パソコンを増設する場合は、増設するパソコンをLAN1～LAN4ジャックに接続してから再起動してください。

IPv4接続が切断されたり、再接続されたりすると、6to4接続のIPv6アドレスも変わることがあります。

■ PPPoE IPv4/IPv6接続の場合

ADSLサービスのPPPリンク上でIPv4/IPv6通信を行う接続は、以下の手順で設定してください。

1 IPv6プロバイダー登録 を選ぶ

2 IPv6プロバイダー登録モニター中で 登録／編集 をクリックする

3 **「PPPoE IPv4/IPv6接続」**を選ぶ

接続モード登録　現在の設定
IPv6ブリッジ接続
トンネル接続
6to4接続
PPPoE IPv4/IPv6接続
Static V6接続

4 **「プロバイダーの名称」**を入力する

半角20文字 (全角10文字) 以内で入力してください。
右の例では、「abcde」を入力しています。

5 プロバイダーから指定がある場合は、**「IPv6 DNSサーバー1」、「IPv6 DNSサーバー2」**を入力する

プロバイダーからの設定情報を参照してください。
元の設定に戻すには、 元に戻す をクリックしてください。

プロバイダー名称
プロバイダー名称　abcde
プロバイダーから指定があるときに入力
IPv6 DNSサーバー1
IPv6 DNSサーバー2
保存して接続設定管理へ　元に戻す　戻る

6 設定を終えたら、 保存して接続設定管理へ をクリックする

接続設定管理画面が表示されます。

7 プロバイダー設定のプロバイダー選択の中から、ステップ4で入力したプロバイダーを選ぶ

8 設定を終えたら、 保存 をクリックする

設定した内容が保存されます。

- **保存中は絶対に電源を切らないでください。保存中に電源を切ると本製品が正常に動作しなくなる可能性があります。**
- IPv4のプロバイダー設定を必ず行ってください。

9 設定画面に 再起動 が表示されたら、それをクリックする

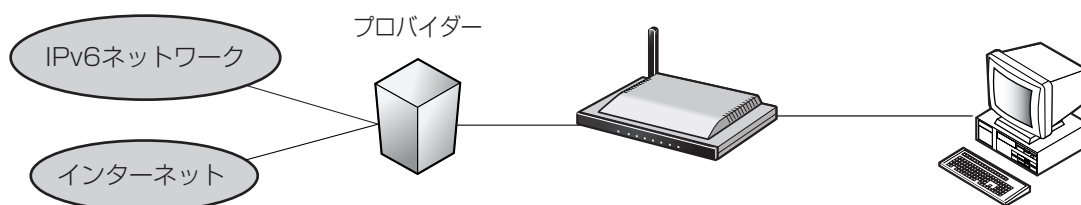
10 パソコンを再起動する

インターネットへの接続を確認してください。
(☞ 56ページ)

- 登録/編集を行った場合、LAN(ホーム)側に接続しているすべてのパソコンを再起動してください。
- 設定完了後パソコンを増設する場合は、増設するパソコンをLAN1〜LAN4ジャックに接続してから再起動してください。

■ Static V6接続の場合

IPv6で直接通信を行います。

Static接続の設定は、以下の手順に従ってください。

1 IPv6プロバイダー登録 を選ぶ

2 IPv6プロバイダー登録モニター中で 登録／編集 をクリックする

3 **「Static V6接続」** を選ぶ

4 **「プロバイダーの名称」** を入力する

半角20文字 (全角10文字) 以内で入力してください。右の例では、「abcde」を入力しています。

5 **「WAN側IPv6アドレス」、「LAN側プレフィックス」、「IPv6デフォルトゲートウェイ」、「IPv6 DNSサーバー1」、「IPv6 DNSサーバー2」** を入力し、プロバイダーから指定がある場合は **「ドメイン名」** を入力する

プロバイダーからの設定情報を参照してください。

プロバイダー名称
プロバイダー名称 abcde
接続先設定
WAN側IPv6アドレス /
LAN側プレフィックス /
IPv6デフォルトゲートウェイ
IPv6 DNSサーバ1
IPv6 DNSサーバ2
プロバイダーから指定があるときに入力
ドメイン名
保存して接続設定管理へ　元に戻す　戻る

つづく

6 設定を終えたら、保存して接続設定管理へ をクリックする

接続設定管理画面が表示されます。

7 プロバイダー設定のプロバイダー選択の中から、ステップ4で入力したプロバイダーを選ぶ

8 設定を終えたら、保存 をクリックする

設定した内容が保存されます。

保存中は絶対に電源を切らないでください。保存中に電源を切ると本製品が正常に動作しなくなる可能性があります。

9 設定画面に 再起動 が表示されたら、それをクリックする

10 パソコンを再起動する

インターネットへの接続を確認してください。
(☞ 56ページ)

- 登録／編集を行った場合、LAN(ホーム)側に接続しているすべてのパソコンを再起動してください。
- 設定完了後パソコンを増設する場合は、増設するパソコンをLAN1～LAN4ジャックに接続してから再起動してください。

■ プロバイダーの登録削除

プロバイダー登録モニターからプロバイダーを削除するには、次の手順に従ってください。

1 削除 したいプロバイダーの登録削除項目の削除を押す

プロバイダーを削除する／しないの確認画面が表示されます。

プロバイダー登録モニター

No.	プロバイダー名称	接続モード	登録編集	使用接続先	登録削除
1	DHCP	DHCP	登録/編集	DHCP接続	削除
2		未登録	登録/編集		削除
3		未登録	登録/編集		削除
4		未登録	登録/編集		削除

2 はい をクリックする

削除を中止する場合は、 いいえ をクリックしてください。

3 設定画面に 再起動 が表示されたら、それをクリックする

インターネットへの接続を確認する

■ 接続の確認

インターネットに接続するための設定が終わったら、ウェブサイトにアクセスしてみてください。ウェブサイトが表示されたら、インターネットに接続されたことになります。

1 ウェブブラウザを起動する

2 ウェブブラウザのアドレスバーにウェブサイトのアドレス（例 http://panasonic.jp）を入力して、 Enter を押す

ウェブサイトが表示されます。

■ ウェブサイトが表示されなかった場合

- ウェブサイトのアドレスがウェブブラウザのアドレスバーに正しく入力されているか、確認してください。
- 本製品に接続しているWANジャック、LANジャックに対応したWANインジケーター、およびLANインジケーターが点灯しているか確認してください。
- モデム(またはONU)→本製品→パソコンの順番で電源を入れたか確認してください。
- ウェブサイトにアクセスするには、ウェブブラウザのプロキシサーバー設定が必要になる場合があります。 (☞ 157ページ)

接続設定を管理する

接続設定管理画面は、登録したプロバイダーの切り替えと、マルチセッションの使用を目的としています。接続設定管理画面では、LAN(ホーム)側からWAN(インターネット)側に、プロバイダー登録された接続するプロバイダーを選びます。
WAN(インターネット)側へ接続するプロバイダーの接続モードには、「DHCP/Static」と「PPPoE」の2種類があります。

■ WAN(インターネット)側接続モードをDHCP/Staticに設定する場合

1 メニュー画面の接続設定管理をクリックする

接続設定管理画面が表示されます。

2 接続モードとして「DHCP/Static」がチェックされていることを確認する

工場出荷時設定では「DHCP/Static」がチェックされています。

3 プロバイダー設定のドロップダウンリストで、プロバイダーを選ぶ

IPv6プロバイダーを設定する場合は、ドロップダウンリストからIPv6プロバイダーを選んでください。

4 [保存] をクリックする

設定が完了したことを知らせる再起動画面が表示されます。

5 [再起動] をクリックする

データ入力欄

プロバイダー設定	使用するプロバイダーを１つ選んでください。プロバイダーの選択は１つのみです。IPv6プロバイダーを登録しているときは、それを選ぶことができます。

■ WAN(インターネット)側接続モードをPPPoEに設定する場合

1 メニュー画面の接続設定管理をクリックする

接続設定管理画面が表示されます。

2 接続モードとして「PPPoE」をチェックする

「プロバイダー設定」が変わり、また、「サブセッションへの切り替えルール」が表示されます。

3 メインセッションのドロップダウンリストで、プロバイダーを選ぶ

メインセッションのプロバイダーは必ず設定してください。

4 サブセッションのドロップダウンリストで、プロバイダーを選ぶ

4、5、6の設定については、プロバイダーとマルチセッションで使用する契約を結んだときにのみ必要になります。

IPv6プロバイダーを設定する場合は、ドロップダウンリストからIPv6プロバイダーを選んでください。

5 **「送信元IPアドレス」**を入力する

6 **「あて先IPアドレスまたはホスト名」**を入力する

7 保存 をクリックする

設定が完了したことを知らせる再起動画面が表示されます。

設定しました。

設定を完了するには再起動する必要があります。
後で再起動する場合は、再起動画面で再起動してください。
今すぐ再起動する場合は、再起動ボタンを押してください。

再起動

8 再起動 をクリックする

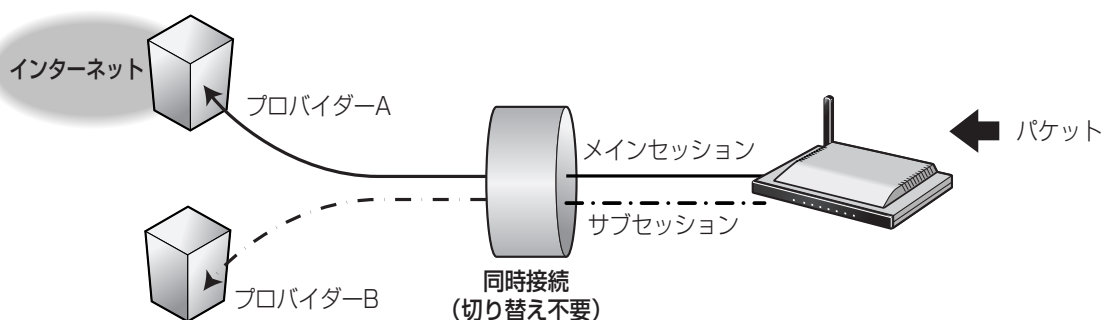
つづく

データ入力欄

プロバイダー設定	メインセッションは必ず設定してください。使用するプロバイダーをメインセッションに設定してください。PPPoEマルチセッション機能を使用する場合は、サブセッションにもプロバイダーを設定する必要があります。IPv6プロバイダーを登録しているときは、それを選ぶことができます。
サブセッションへの切り替えルール	通常のインターネットへの接続は、メインセッションに設定したプロバイダーが使用されます。条件に一致した通信が検出された場合には、サブセッションに設定したプロバイダーが使用されます。 送信元IPアドレス欄には、LAN(ホーム)側からインターネットへのパケットの送信元IPアドレス（サブセッションを利用するLAN(ホーム)側のホストのIPアドレス）を設定します。 あて先IPアドレスまたはホスト名欄には、LAN(ホーム)側からWAN(インターネット)側へのパケットのあて先IPアドレスまたはホスト名（WAN(インターネット)上のどのホストへの通信がサブセッションを利用するか）を設定します。

■ PPPoEマルチセッション機能（IPv4のみ）

本製品はPPPoEマルチセッション機能に対応しており、同時に2つのPPPoE接続を接続することができます。プロバイダーを2つ設定することにより、接続の切り替えをしなくても指定したプロバイダーを利用してインターネットへ接続することができます。フレッツでは複数のセッションを利用することができます。フレッツ・スクウェアについては61ページを参照してください。

PPPoEマルチセッション機能を使用するためには、この機能に対応した回線接続業者またはプロバイダーと別途契約する必要があります。詳細は各回線接続業者またはプロバイダーにお問い合わせください。

- みえますねっと(☞ 79ページ)は、メインセッションのみ有効です。
- IPアドレス通知はメインセッションのみ有効です。

<PPPoEマルチセッション設定例>

本製品では、PPPoEマルチセッション機能を使用することで、通常のインターネット接続をしたままフレッツ・スクウェアなどへの接続をすることができます。この設定を行うことにより、通常のインターネット接続とフレッツ・スクウェアなどへの接続を、自動的に切り替えることができます。

PPPoEマルチセッションを利用するには、メインセッションの登録が必要です。
プロバイダー経由の通常のインターネット接続用設定は必ずメインセッションに設定してください。
メインセッションの登録は、下記を参照してください。

- **端末型PPPoE接続の場合** (☞ 32ページ)
- **LAN型PPPoE接続の場合** (☞ 39ページ)

メインセッション、サブセッションの両方にLAN型PPPoEを設定することはできません。LAN型PPPoEを設定するときは、いずれか一方に設定してください。

IPアドレス指定方法

「送信元IPアドレス」および「あて先IPアドレス」の指定方法です。

IPアドレス	説明
＊	すべてのIPアドレス
192.168.1.3	特定のIPアドレス
192.168.1.0／24	192.168.1.0～192.168.1.255までのIPアドレス (24ビットマスク)
192.168.1.3-192.168.1.33	ハイフン“-”区切り: 192.168.1.3～192.168.1.33までのIPアドレス
192.168.1.3,192.168.1.8, 192.168.1.3-192.168.1.33, 192.168.1.0／24	コンマ“,”区切り: コンマで区切ることでそれぞれを4つまで指定できます いずれもスペースなし

ホスト名指定方法

「あて先ホスト名」としてのみ使用できます。またIPアドレスを用いた指定方法との併用はできません。

ホスト名	説明
.jp	トップレベルドメインのみ指定 日本(jp)サイトすべて
.co.jp	セカンダリレベルドメインまで指定 最後に“co.jp”がつくサイトすべて
www.panasonic.co.jp	“www.panasonic.co.jp”のみ
.www.panasonic.co.jp	“host1.www.panasonic.co.jp”、“host2.www.panasonic.co.jp” “www.panasonic.co.jp”には該当しない 上の例と“.”(ドット)の有無による違いに注意
www.＊.co.jp	第3レベルドメインを除き、第4、第2、第1レベルドメインを指定 第4レベルドメインが"www"、かつ、第2レベルドメインまでが"co.jp"であるサイトすべて

＜フレッツ・スクウェアの設定例＞

プロバイダーのPPPoEアカウントを1つしかもっていなくても、フレッツユーザーであればフレッツ・スクウェアのPPPoEアカウントを無料で利用できます。

1 プロバイダー登録 を選ぶ

2 プロバイダー登録モニター中で 登録／編集 をクリックする

3 接続モード登録画面で端末型のPPPoE接続をクリックする

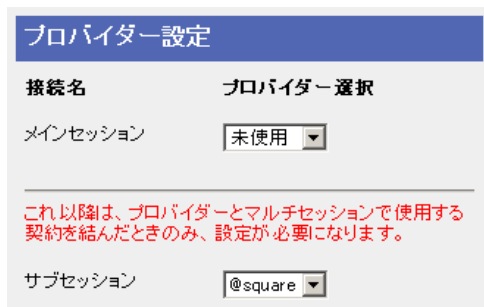
4 プロバイダーの名称（任意の文字列）、ユーザー名、パスワード欄にそれぞれ入力する

プロバイダーの名称
プロバイダーの名称
プロバイダー登録
ユーザー名
パスワード
プロバイダーから指定があるときに入力
サービス名
アクセス
コンセントレーター名
DNSサーバー1
DNSサーバー2
ドメイン名

平成16年12月現在

設定項目	プロバイダーの名称※	ユーザー名	パスワード
NTT東日本フレッツ・スクウェア	@square	guest@flets	guest
NTT西日本フレッツ・スクウェア	@square	flets@flets	flets

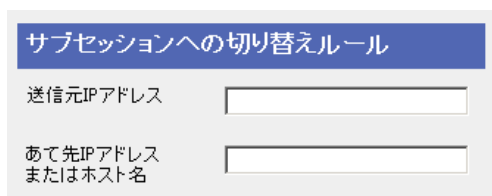
※ ここに示しているプロバイダーの名称は例です。任意の文字列を設定することができます。

つづく

5 設定を終えたら、［保存して接続設定管理へ］をクリックする

保存して接続設定管理へ　元に戻す　戻る

接続設定管理画面が表示されます。

6 プロバイダー設定欄のサブセッションに、手順4で登録した@squareを選ぶ

プロバイダー設定

接続名　プロバイダー選択

メインセッション　未使用

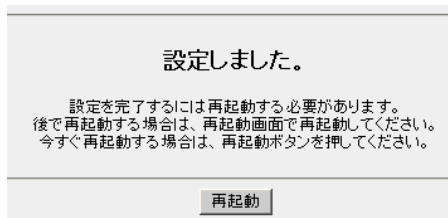
これ以降は、プロバイダーとマルチセッションで使用する契約を結んだときのみ、設定が必要になります。

サブセッション　@square

7 サブセッションへの切り替えルール欄に下表に示している設定値を入力する

サブセッションへの切り替えルール

送信元IPアドレス

あて先IPアドレスまたはホスト名

送信元IPアドレス	＊
あて先IPアドレスまたはホスト名	.flets

8 設定を確認したら、［保存］をクリックする

内容が保存されます。

保存中は絶対に電源を切らないでください。保存中に電源を切ると本製品が正常に動作しなくなる可能性があります。

9 設定画面に、［再起動］が表示されたら、それをクリックする

10 ウェブブラウザのアドレスバーにhttp://www.flets/を入力してフレッツ・スクウェアのウェブサイトが表示できれば正常にサブセッションが確立しています

オプション設定画面にアクセスして、DNSリレーが「使用する」になっていることを確認してください。（☞ 110ページ）

フレッツ・スクウェアに関しては、以下のウェブサイトを参照してください。
NTT東日本ウェブサイト　http://www.ntt-east.co.jp/flets/
NTT西日本ウェブサイト　http://www.ntt-west.co.jp/flets/

カメラを使う

本製品に接続したカメラの設定を行います。通常は、カメラ自動登録機能によりカメラ名やポート番号、IPアドレスを自動で設定するため、設定の必要はありません。カメラ名を変更する場合は、65ページを参照してください。またカメラのネットワーク設定を手動で行う場合は、66ページを参照してください。

■ カメラの自動登録機能の設定

カメラの自動登録機能の設定

◉ 使用する　○ 使用しない

--[V4カメラの自動登録機能の設定]------------------------------------

利用可能なアドレス範囲　192.168.0.151 - 192.168.0.166

カメラに設定するポート番号　○ 単一指定　◉ 範囲指定

利用可能なポート範囲　60001 - 60016

データ入力欄

カメラの自動登録機能の設定	「使用する」または「使用しない」を選んでください。
利用可能なアドレス範囲	カメラに割り振る連続したアドレス範囲を1つ指定します。 ● LAN型接続時は、プロバイダーより割り振られるグローバルアドレスのうち、カメラまたはパソコンとして利用できるアドレス範囲(☞ 39ページ)の中のうちでも設定できます。 ● DHCP／PPTPサーバーなどほかのサーバーが割り振るアドレスと重複しないようご注意ください。 ● 工場出荷時設定は192.168.0.151－192.168.0.166です。
カメラに設定するポート番号	「単一指定」または「範囲指定」を選んでください。 ●「範囲指定」をチェックすると、「利用可能なポート範囲」の値が自動で割り振られます。 ●「単一指定」は、次のような接続形態において、使用することができます。 (1) プロバイダーへの接続モードがLAN型 (2) アドレス変換を使用しないで、WAN側を社内ネットワークなどに接続して使用する場合 (3) WAN側を接続しないでLAN内でのみ使用する場合
利用可能なポート範囲	カメラのポート番号を指定してください。 ●「カメラに設定するポート番号」で「範囲指定」を選んだ場合、連続したポート番号範囲1つを指定できます。上記の利用可能なアドレス範囲で指定した数のポート番号数が必要です。利用できるポート番号範囲から指定してください。 ●「カメラに設定するポート番号」で「単一指定」を選んだ場合、固定ポート番号を1つ指定してください。 ● 工場出荷時設定は60001－60016 です。

カメラを自動登録する（カメラおまかせってい）

本製品に当社製ホームネットワークカメラ(別売品)を接続し、カメラの電源を入れてカメラを工場出荷時設定に戻すと、本製品は、IPアドレスやサブネットマスク、無線のセキュリティなどの設定を自動で行います。本製品とカメラが通信を行い、自動的にネットワークの設定を行います。そのあと、カメラ画像がカメラモニター画面に登録されます。

<設定される項目>

本製品	静的IPマスカレード（ポートフォワーディング） カメラ登録 カメラモニター画面配置
カメラ	ポート番号（IPv4） IPアドレス（IPv4） サブネットマスク、プレフィックス長 デフォルトゲートウェイ DNSサーバーアドレス SSID（無線LANタイプのみ） 暗号化キー（無線LANタイプのみ）

■ 当社対応製品 (別売品) (平成16年12月現在)

ホームネットワークカメラ

屋内タイプ

BL-C30　(パン／チルト・無線)
BL-C10　(パン／チルト)

無線LANアダプター

BL-WA30

■ カメラ自動登録機能を使わずにカメラを接続する

- すべてのカメラを手動で登録する場合は、「カメラの追加登録」(☞ 66ページ）を参照のうえ、設定してください。
- 特定のカメラを手動で登録する場合、カメラのネットワーク設定で、「セットアップソフトウェアからの設定」の有効のチェックをはずしてください。詳細はカメラ取扱説明書の「ネットワーク設定」を参照してください。

■ 自動登録されたカメラの設定変更

1 設定画面上の **カメラ設定** をクリックする

2 設定するカメラの**変更／削除**をクリックする

3 **カメラ名、PPPoEマルチセッションの場合のセッション選択**のうち必要な項目を設定し、 **更新** をクリックする

登録されているカメラを削除する場合は **削除** をクリックしてください。

4 設定を終えたら、 **保存** をクリックする

設定した内容が保存されます。

5 設定画面に **再起動** が表示されたら、それをクリックする

設定を変更したあとは、再起動してください。

- カメラ側でインターネットに対する公開／非公開の設定があるタイプのカメラにおいては、公開／非公開に関してカメラ側の設定に従います。
- 自動登録されたカメラのポート番号やIPアドレスを変更することはできません。
- 「画像確認」で確認をクリックすると、カメラの画面を表示します。ただし、設定によってはカメラ画像を表示できないことがあります。

■ カメラの追加登録(カメラを手動で追加登録する)

カメラの追加登録は、次の手順に従ってください。

1 「カメラ名変更とカメラの追加登録・削除」で 追加 をクリックする

2 必要項目を設定し、 追加 をクリックする

3 設定を終えたら 保存 をクリックする

設定した内容が保存されます。

4 設定画面に 再起動 が表示されたら、それをクリックする

5 68ページの方法に従って、追加されたカメラをカメラモニター画面に追加する

- カメラを追加登録した場合、カメラ側の設定も変更してください。詳細は、カメラの取扱説明書を参照してください。
- 静的IPマスカレード(ポートフォワーディング)などの設定が必要です。83ページを参照のうえ、手動で設定してください。また、UPnP™上位ルーターを使用している場合には、上位ルーターに対するルーティング設定、アドレス変換を「使用しない」に設定している場合にも、接続される周辺ルーターに対するルーティング設定が必要となります。
- カメラを追加登録した場合、カメラモニター画面配置の設定が必要です。68ページを参照のうえ、手動で設定してください。
- オプション設定での「IPアドレス(LAN側)DHCPサーバー」におけるDHCPの設定で指定されるDHCPサーバーの「利用可能なアドレス範囲」、および、「VPN設定」での基本画面における「PPTPサーバーの設定」で指定されるPPTPサーバーの「利用可能なアドレス範囲」と重複したIPアドレスを、カメラの自動設定に用いるIPアドレスの範囲として設定してはいけません。

つづく

データ入力欄

カメラ名		半角英数で16文字以内、全角文字で8文字以内で入力してください。
カメラの配置		カメラの配置に従って、LAN側かWAN側にチェックを入れてください。
WAN側へのカメラ画像公開 PPPoEマルチセッションの場合		カメラ側でインターネット公開／非公開の設定がないタイプのカメラにおいては、公開する／公開しないの設定ができます。また、PPPoEマルチセッションの場合は公開するセッションを選ぶことができます。
カメラの設定	ポート番号	カメラのポート番号を入力してください。
	IPアドレス	カメラのIPアドレスを入力してください。
	ホスト名	カメラの位置でWAN側を選んだときにホスト名による指定ができます。

カメラを手動で追加登録する場合、さらに、設定するカメラに対する本製品のフィルタリング設定(☞ 98ページ)やアドレス変換(☞ 81ページ)などを設定しなければなりません。カメラが自動登録される場合には、フィルタリング設定もアドレス変換も自動で設定されます。

■ カメラモニター画面配置

カメラモニター画面の画面表示形式や画面配置の設定を行います。

1 カメラモニター画面配置 をクリックする

2 「カメラモニター画面表示形式」で**「カメラ名と静止画（自動更新)」、「カメラ名と静止画」、「カメラ名のみ」**の中から選ぶ

3 ドロップダウンリストからカメラを選び、配置したいカメラ画面枠をクリックする

選んだカメラ画面枠はオレンジに表示されます。カメラモニター画面からカメラをはずす際は、**「カメラモニター画面からカメラをはずす」**を選び、カメラ画面枠をクリックしてください。

現在の選択をキャンセルするには、 元に戻す をクリックしてください。

4 設定を終えたら、 保存 をクリックする

元の設定に戻すには、 元に戻す をクリックしてください。

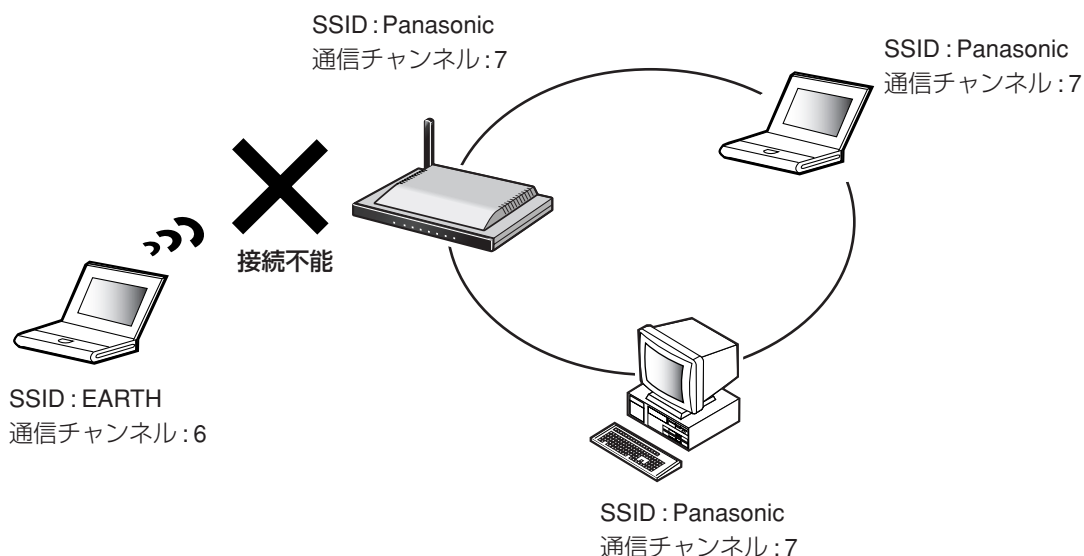
5 設定画面に、 再起動 が表示されたら、それをクリックする

登録されたカメラ画面枠は緑に表示されます。

データ入力欄

カメラモニター画面表示形式	カメラの画面表示形式を「カメラ名と静止画（自動更新)」、「カメラ名と静止画」、「カメラ名のみ」の中から選びます。
カメラモニター画面配置	カメラモニター画面のカメラ画像の配置を変更したり、任意のカメラをカメラモニター画面へ登録します。最大16台のカメラ画像をカメラモニター画面で一覧表示することができます。

無線LANを使う

無線設定画面では、無線LANに接続するための設定やセキュリティの設定を行います。無線LANでは、テレビやトランシーバーと同じように電波を使い、通信チャンネルを選んで通信します。「802.11b」、「802.11b/g」、「802.11g 専用」、「802.11a」、「Super A（圧縮なし）」、「Super A（圧縮あり）」、「Super G（圧縮なし）」、「Super G（圧縮あり）」の8つの通信モード※1はそれぞれ使用する帯域や通信速度が異なっています。工場出荷時設定は「802.11b/g」です。また、ネットワークに名前(SSID)をつけ、同じSSIDと同じ通信チャンネルの機器同士でのみ接続することができます。無線LANに接続する機器には同じSSIDと通信チャンネル※2を設定してください。

※1 802.11aの屋外での使用は法律により禁止されています。
※2 本製品に接続する無線機器は、本製品と同じSSIDが設定されていれば、通信チャンネルを自動的に検索し、通信することができます。

- **工場出荷時設定では、機器固有のSSIDと英数13文字128 bit暗号化キーが設定されています。SSIDと英数13文字128 bit暗号化キーの工場出荷時設定は、本製品背面に記載してあります。**
- 当社製無線LANアダプターをリピーター(電波中継器)として使用すると、無線LANの伝達距離を約2倍に延長することができます。本製品と無線カメラの間の距離が離れていたり、途中に障害物などがある場合に、当社製無線LANアダプターをリピーターモードに設定して中間地点に設置すれば良好な電波状態で通信できるようになります。リピーターは無線カメラを3台まで中継できます。
- 当社製無線LANアダプターがクライアントモードで本製品と無線通信していても、当社製無線LANアダプターのLANジャックに接続されている有線機器からのデータ通信が一定期間行われないと、本製品は無線通信を強制切断します。これは、本製品がほかの無線通信を優先させるため、通信していない無線機器を切断するので、無線通信の負荷を軽減させることができます。
- 当社製無線LANアダプターとの自動設定機能の手順については、無線LANアダプターのかんたんガイドを参照してください。
- 通信モードに「802.11a」、「Super A（圧縮なし）」、「Super A（圧縮あり）」、「Super G（圧縮なし）」、「Super G（圧縮あり）」を使用している場合、または暗号化方式が「WPA」になっている場合、当社製無線LANアダプター、ホームネットワークカメラは自動設定されません。自動設定を行うには、通信モードを「802.11b」または「802.11b/g」、暗号化方式を「WEP」にしてください。(☞ 次ページ)

つづく

1 設定画面上の 無線設定 をクリックする

2 入力欄にSSIDを入力し、**「通信チャンネル」**を選ぶ

「無線ステルス機能」の設定については、71ページを参照してください。
元の設定に戻すには、 元に戻す をクリックしてください。
本製品に接続する無線機器にも同じSSIDを入力してください。
工場出荷時に設定しているSSIDの工場出荷時設定は本製品背面に記載されています。
それぞれの入力欄については、71ページを参照してください。

3 設定を終えたら、 保存 をクリックする

設定した内容が保存されます。

4 設定画面に、 再起動 が表示されたら、それをクリックする

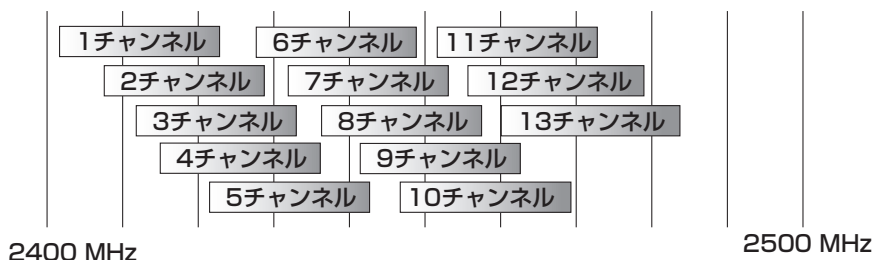
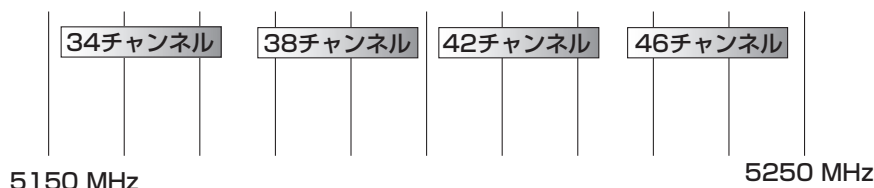
- 無線ステルス機能を「使用しない」に設定した場合、セキュリティが弱くなります。
- 無線機器側で使用している無線LANカードによっては、使用できる通信チャンネルに制限のあるものがあります。無線LANカードの通信チャンネルの範囲を確認して、本製品の通信チャンネルを設定してください。
- 無線カメラなどを自動登録したあとに本製品のSSIDを変更した場合は、無線カメラなどの設定を合わせる必要があります。

つづく

データ入力欄

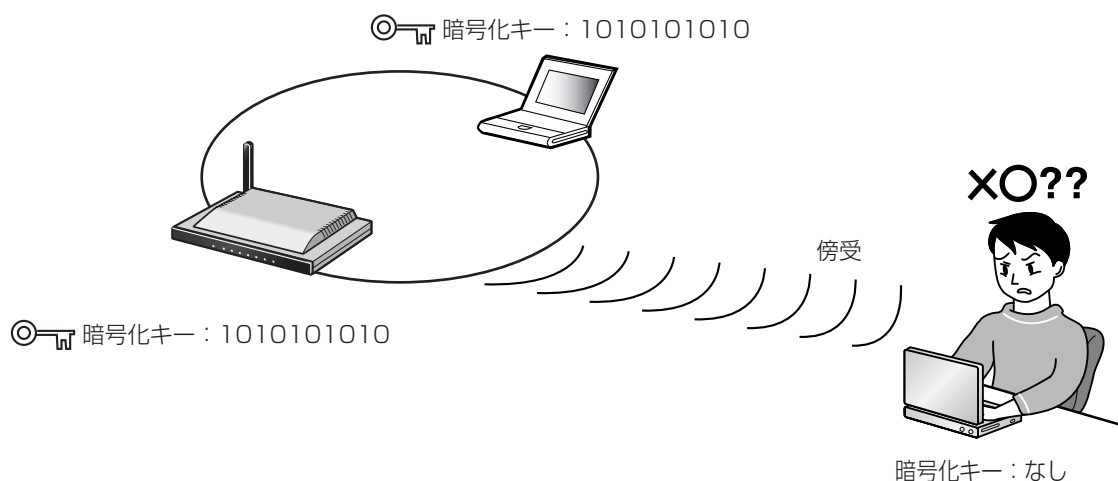
通信モード	通信方式を、無効、「802.11b」、「802.11b/g」、「802.11g専用」、「802.11a」、「Super A（圧縮なし）」、「Super A（圧縮あり）」、「Super G（圧縮なし）」、「Super G（圧縮あり）」から選ぶことができます。 ● 無効は、無線通信を行わない場合に選びます。 ●「802.11b」は、2.4 GHz帯で通信を行います。対応製品が豊富かつ安価です。手軽に利用できるだけでなく、すでに広く普及しているので、お手持ちの無線機器を活用したいときなどに便利です。 ●「802.11b/g」は、2.4 GHz帯で通信を行います。802.11bと802.11gの特長を兼ねそなえ、両方の無線LAN規格に対応しています。既存の無線LAN環境に導入しやすい通信方式です。 ●「802.11g専用」は、802.11g通信のみを行います。本製品の通信モードも、「802.11g専用」に設定すれば、「802.11b/g」の混在モードはサポートしないので、本来の802.11gの性能が発揮されます。※1 802.11bより速度が速く、障害物に強い規格なので、異なるフロア間での通信などに便利です。 ※1 802.11g専用を使用しても、ほかの2.4 GHz帯の無線機器(802.11b無線機器を含む)が存在するとその影響を受けて通信速度が遅くなります。 ●「802.11a」は、5.2 GHz帯で通信を行います。ほかの家電製品と干渉する可能性が低く、高速、かつ、安定した通信を行います。障害物が少ない場合、802.11gで速度が遅い場合、また、大容量動画データの安定したストリーミング再生を行う場合などに便利です。 ●「Super A」、「Super G」は無線通信を行う前に送信するデータを圧縮し、受け取った側で圧縮されたデータを展開することで、より短い時間でデータを送信できます。「圧縮あり」はリアルタイムでデータを圧縮して送信します。圧縮効果のあるテキストデータやビットマップデータなどを高速転送できます。
SSID	無線LANでは、ネットワークに名前をつけます。この名前をSSIDと呼びます。SSIDは、無線LANに接続できる各機器に設定し、同じSSIDをもつ機器同士でのみ通信ができます。SSIDの入力では、次の規則に従ってください。（工場出荷時設定で機器固有のSSIDが入力されています。本製品背面に記載されています。） ● 半角英数字しか入力できません。 ● 英字の大文字と小文字は区別されます。 (例) : "ABC" と "abc" は異なる名前と認識される ● 32文字まで入力できます。
無線ステルス機能	無線LAN機器がネットワークを検知できるように、ネットワークの識別子であるSSIDを一定時間ごとに周囲に発信する機能があります。「使用しない」を選ぶと、無線LAN機器は、容易にネットワーク内の機器を検知することができます。しかし、不正規のユーザーも容易にネットワーク内の機器を発見して接続を試みることができるため、セキュリティ上の弱点となる可能性があります。そこで、無線ステルス機能を「使用する」を選ぶことにより、ネットワーク内の機器を容易に検知されないように本製品を使用することができます。「使用する」に設定した場合、ANYキーによる接続が拒否されます。工場出荷設定では、「使用する」が選ばれています。

つづく

通信チャンネル	ネットワーク内で通信するチャンネルを設定します。802.11bまたは802.11gの場合、1～13の中から選びます。（工場出荷時設定では、802.11b/gの7が選ばれています。また、14チャンネルには対応していません。）802.11aの場合、34、38、42または46の中から選びます。複数の無線LANで、通信チャンネルが重なると通信速度が下がる場合があります。その場合は、通信チャンネルが重ならないように通信チャンネルを変更してください。

本製品と無線機器側で同じSSIDを設定する必要があります。

必要に応じて「暗号化」や「MACアドレスフィルタリング」を設定してください。通信データを暗号化するには、「無線設定」画面上の「暗号化」をクリックしてください。（☞ 73ページ）本製品に登録した無線機器以外が接続できないようにするには、「MACアドレスフィルタリング」をクリックしてください。（☞ 78ページ）

■ 暗号化設定

無線LAN内で、通信するデータを暗号化することができます。暗号化を行うと、万一無線LANのデータを、他人に読まれても解読することが困難になります。暗号化は、無線LANのすべての機器に同じ暗号化キーを登録して行います。
暗号化を必ず設定してください。暗号化設定をせずに無線LANを使用すると、第三者に通信内容を盗聴されたり、パソコンに侵入されインターネットを不正使用されるなどの危険があります。
暗号化設定時の認証方式として、Shared Key方式だけでなく、Open System方式にも対応しています。認証方式の切り替えは、本製品が機器に合わせて自動で行います。

- **工場出荷時設定では、機器固有のSSIDと英数13文字128 bit暗号化キーが設定されています。SSIDと英数13文字128 bit暗号化キーの工場出荷時設定は、本製品背面に記載してあります。**
- WEP方式には、「16進10文字 64 bit」、「16進26文字 128 bit」、「16進32文字 152 bit」、「英数5文字 64 bit」、「英数13文字 128 bit」、「英数16文字 152 bit」の6種類があります。
- カメラはWPA方式に対応していませんので、カメラを接続するときはWEP方式を選んでください。

カメラなどを自動登録したあとに本製品の暗号化設定を変更した場合は、カメラなどの設定を合わせる必要があります。

1 [暗号化] をクリックする

2 「暗号化方式」のドロップダウンリストから**「なし」**または**「WEP」、「WPA-PSK/WPA2-PSK」**を選ぶ

「暗号化なし」を選んだときは、[保存] をクリックしてください。

暗号化方式の設定	
暗号化方式	WEP

つづく

＜「WEP」 を選んだ場合＞

3 WEPキー1～WEPキー4のそれぞれのドロップダウンリストから、**「16進10文字 64 bit」、「16進26文字 128 bit」、「16進32文字 152 bit」、「英数5文字 64 bit」、「英数13文字 128 bit」、「英数16文字 152 bit」**のうちいずれかを選ぶ

4 WEPキー1～WEPキー4のそれぞれの空欄に、ドロップダウンリストで選んだ項目の文字数分を16進数(半角英数字で"0"～"9"、"A"～"F"または"a"～"f")または英数字で入力し、使用するWEPキー番号にチェックを入れる

(例)

WEPキー1	0123456789abcdef012345abc	16進26文字 128 bit
WEPキー2	0123456789abcdef0123456789abcde	16進32文字 152 bit
WEPキー3	012y	英数5文字 64 bit
WEPキー4	0123456789uvwxy	英数16文字 152 bit

- **設定内容は、本製品を再起動すると＊（アスタリスク）で表示され、わからなくなります。必ずメモに記録しておき大切に保管してください。**
- 接続する無線機器にも同じWEPキー1～WEPキー4を入力し、ステップ4でチェックを入れた同じWEPキー番号を選んでください。データ入力欄については次ページを参照してください。

- Windows XPでは暗号化キーは、「キーのインデックス」という名称になっています。
- 本製品と当社製無線LANアダプターでは128 bitのWEPキーを4つ設定できます。自動設定で引き継がれる128 bitのWEPキーはWEPキー1だけです。

5 **保存** をクリックする

6 設定内容を確認のうえ、 **再起動** をクリックする

BL-C30の無線LANの各項目は、次の項目に相当します。

40 bitのキー入力	16進10文字 64 bit
128 bitのキー入力	16進26文字 128 bit
40 bitのパスワード入力	英数5文字 64 bit
128 bitのパスワード入力	英数13文字 128 bit

つづく

データ入力欄

暗号化方式	「なし」、「WEP」、「WPA-PSK/WPA2-PSK」のいずれかを選びます。「なし」→「WEP」→「WPA-PSK/WPA2-PSK」の順で安全性が高まります。(工場出荷時設定では「WEP」が選ばれています。)
暗号化キーの設定	64 bit→128 bit→152 bitの順で安全性が高まりますが、反対に通信速度が若干低下します。また、Windows XPでは、「64 bit」は「40 ビット(10桁)」、「128 bit」は「104 ビット(26桁)」と表記されています。 (工場出荷時設定では「WEPキー1」の「英数13文字 128 bit」が選ばれています。)

無線カメラなどを自動登録したあとに本製品の暗号化設定を変更した場合は、無線カメラなどの設定を合わせる必要があります。

＜「WPA-PSK/WPA2-PSK」 を選んだ場合＞

3 ネットワークキーに、8〜63文字の英数記号または64文字の16進数で入力する

- **設定内容は、本製品を再起動すると＊（アスタリスク）で表示され、わからなくなります。必ずメモに記録しておき大切に保管してください。**
- 接続する無線機器にも同じネットワークキーを入力してください。データ入力欄については次ページを参照してください。

更新間隔は、「AUTO」または「WPA-PSK(TKIP)」が選ばれているときのみ有効です。

4 **「更新間隔」**と**「データの暗号化」**を設定する

5 [保存] をクリックする

6 設定内容を確認のうえ、[再起動] をクリックする

つづく

データ入力欄

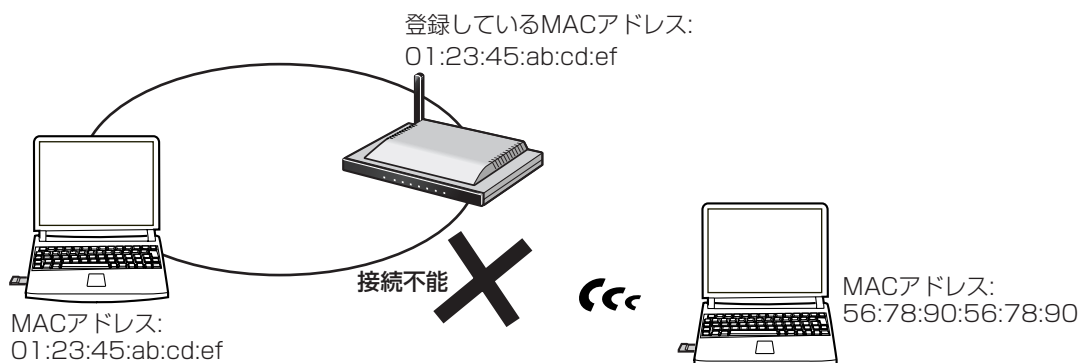
暗号化方式	「なし」、「WEP」、「WPA-PSK/WPA2-PSK」のいずれかを選びます。「なし」→「WEP」→「WPA-PSK/WPA2-PSK」の順で安全性が高まります。 (工場出荷時設定では「WEP」が選ばれています。)
ネットワークキー	8～63文字の英数記号または64文字の16進数で入力してください。暗号化する場合、通信するパソコンに同じネットワークキーを設定する必要があります。設定したネットワークキーは1度しか表示されませんので、必要な場合はメモをとることをおすすめします。
更新間隔	暗号化キーを更新する時間間隔を設定します。 ● 30～604800秒の間で設定してください。最大値の604800秒は、1週間のことです。
データの暗号化	データの暗号化方式を以下の3つから選ぶことができます。 ● WPA-PSK(TKIP) パケットごとに暗号化キー（WEP）を変更する機能やメッセージごとに改ざんを防ぐ機能があるため、WEPよりさらに強固なセキュリティを実現します。 ● WPA2-PSK(AES) 米商務省技術標準局（NIST）が選定した次世代の暗号化方式です。TKIPよりさらに強固な暗号化を行うことができます。 ● AUTO TKIPまたはAESが自動的に選ばれます。

無線カメラなどを自動登録したあとに本製品の暗号化設定を変更した場合は、無線カメラなどの設定を合わせる必要があります。

本製品が「WPA-PSK(TKIP)」を使用している場合、接続する無線機器側はネットワークキーが一致していれば、TKIPまたはAESのどちらの暗号化方式でも本製品に接続できる場合があります。

■ MACアドレスフィルタリング登録

本製品に登録していないパソコンから本製品に接続できないようにします。各パソコンのLANカードには、そのLANカードに固有のMACアドレスが登録されています。そのMACアドレスの値を「MACアドレスフィルタリング」に登録すると、登録したMACアドレスをもつパソコン以外は接続できなくなります。各パソコンのMACアドレスの確認のしかたは「パソコンのIPアドレスやMACアドレスを確認するには」(☞ 158ページ)を参照してください。

当社製無線ホームネットワークカメラを使用している場合の設定については、パナソニックのサポートウェブサイト（http://panasonic.co.jp/pcc/products/hnetwk/support/）を参照してください。

1 [MACアドレスフィルタリング] をクリックする

2 **「使用する」**を選ぶ

3 「現在の設定」でNo. の**「追加」**をクリックする

MACアドレスフィルタリング　○使用する ◉使用しない
MACアドレスフィルタリングの"使用する"を選択すると、下記で登録した無線端末(ネットワークカメラやパソコン)のみ本製品と通信できます。

現在の設定
操作項目をクリックすると各設定画面が開き、変更/削除/追加ができます。

No.	操作	MACアドレス
	追加	

4 MACアドレスをデータ入力欄に入力する

半角数字とA～Fまたはa～fを2文字ずつ「：」で区切って、「01:23:45:ab:cd:ef」のように入力してください。

MACアドレス
[追 加] [戻 る]

5 [追加] をクリックする

6 [保存] をクリックする

7 設定内容を確認のうえ、[再起動] をクリックする

みえますねっとを使う

WAN(インターネット)側からカメラ画像を見るには、みえますねっと設定を利用します。みえますねっとサービスからURLを取得して、カメラモニター画面にアクセスしてカメラ画像を見ることができます。みえますねっと設定を利用してWAN側からカメラ画像を見るには、次の手順に従ってください。

みえますねっとサービスは有料サービスです。次の手順は、みえますねっとサービスを有料にて使用される場合のみ行ってください。

- Static接続でインターネット接続している場合は、本製品の「基本設定」にて登録したIPアドレスを使用してカメラモニター画面にアクセスできます。みえますねっとサービスに登録する必要はありません。
- PPPoE接続の場合、メインセッションにのみ、みえますねっとは有効です。

1 設定画面上の **みえますねっと設定** をクリックする

2 **「使用する」**を選ぶ

3 Eメールアドレス入力欄に登録用の**Eメールアドレス**を入力する

カメラをすでにみえますねっとサービスに登録している場合は、本製品にみえますねっと設定を行わないでください。

連絡先Eメールアドレスを入力するとみえますねっとサーバーから登録のご案内メールが送付されます。

4 **保存** をクリックする

5 設定画面に **再起動** が表示されたら、それをクリックする

トップページが表示されます。

6 **かんたん設定** をクリックする

かんたん設定画面が表示されます。

つづく

7 設定画面上の［みえますねっと設定］をクリックする

仮登録用の取得URLとみえますねっとサービスの利用者登録ページへのリンクが表示されます。

- 取得URLとみえますねっとサービスの利用者登録ページへのリンクが表示されるまで数十分かかることがあります。
- PPPoE(マルチセッション)のときは、メインセッションのIPアドレスがみえますねっとサーバーに登録されます。

8 みえますねっとサービスの利用者登録ページへのリンクをクリックする

9 「みえますねっと」の登録手順に従って、本製品を「みえますねっと」に登録する

10 インターネットに接続できるパソコンのウェブブラウザに、「取得URL」に表示されているURLを入力する

(例：http://camXXXX.miemasu.net)

カメラモニター画面が表示されます。

「取得URL」はみえますねっとサービスに登録したあとに利用できるようになります。みえますねっとサービスの利用者登録ページで登録してください。

拡張機能を使う

インターネットから本製品にアクセスする

アドレス変換画面では、WAN(インターネット)側のグローバルアドレスとプライベートアドレスを相互変換して、インターネットの端末から本製品のネットワークにアクセスするための詳細な設定を行います。メールサーバーを立ち上げるときなどIPマスカレード機能、静的IPマスカレード機能を有効にする場合に、設定してください。UPnP™対応アプリケーション(Windows／MSN Messengerなど)を利用する場合は、113、145ページを参照してください。

1 設定画面上の [アドレス変換] をクリックする

2 「有効／無効の設定」で**「使用する」**か**「使用しない」**を選ぶ

3 設定を終えたら、[保存] をクリックする

設定した内容が保存されます。

4 設定画面に、[再起動] が表示されたら、それをクリックする

WAN(インターネット)側の1つのグローバルアドレスを利用して静的IPマスカレードの設定をする場合は、**「端末型」**をクリックしてください。端末型のアドレス変換については83ページを参照してください。WAN(インターネット)側の複数のグローバルアドレスを利用してアドレス変換する場合は、**「LAN型」**をクリックしてください。LAN型のアドレス変換については88ページを参照してください。

アドレス変換を行った場合、本製品に接続しているパソコンのネットワーク設定も行い、パソコンを再起動してください。

つづく

拡張機能を使う

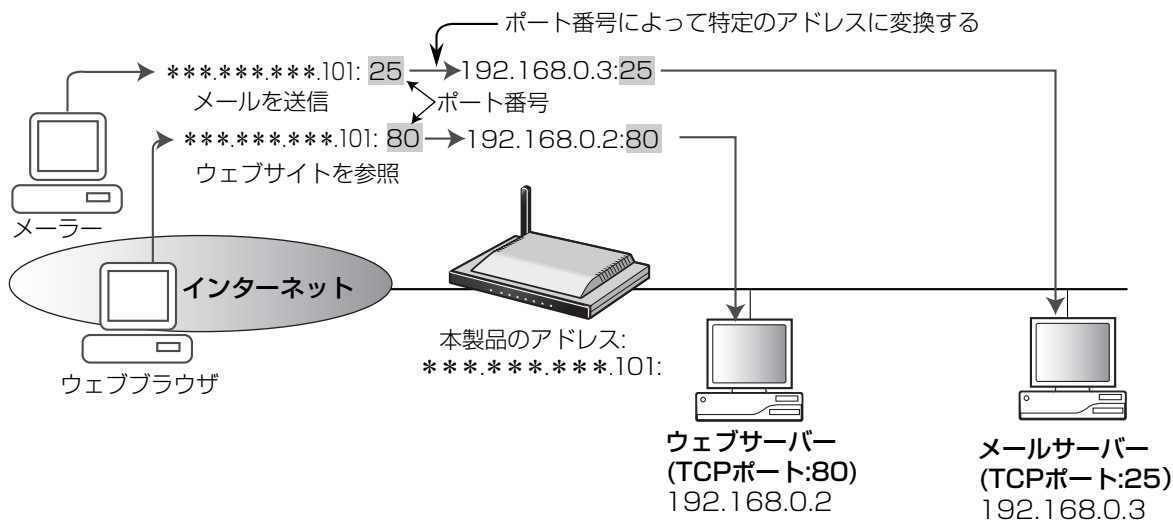
データ入力欄

	DHCP/Static接続
DHCP/Static	IPマスカレード、静的IPマスカレード、静的NAT機能を有効にするときに設定します。これらの機能を使用する場合には、「使用する」チェックを入れてください。
PPPoE接続	
メインセッション	IPマスカレード、静的IPマスカレード、静的NAT機能を有効にするときに設定します。これらの機能を使用する場合には、「使用する」チェックを入れてください。
サブセッション	PPPoEマルチセッション機能を使用しているとき、サブセッションのIPマスカレード、静的IPマスカレード、静的NAT機能を有効にするときに設定します。これらの機能を使用する場合には、「使用する」チェックを入れてください。

■ 端末型アドレス変換

静的IPマスカレード（ポートフォワーディング）

WAN(インターネット)側のパソコンからアプリケーションを使ってLAN(ホーム)側のサーバーに通信が行われると、パケットが本製品に送られます。パケットにはアプリケーションが使用するポート番号がついており、本製品がパケットを特定のパソコンに転送します。静的IPマスカレードの機能を利用するには、アプリケーションが利用するポート番号※を調べ転送対象ポート入力欄に入力し、転送先IPアドレス入力欄に対応するパソコンのIPアドレスを入力してください。

※主なアプリケーションとポート番号について
ウェブサーバー：TCP 80番、FTPサーバー：TCP 20番と21番、
Telnet：TCP 23番、SMTPサーバー：TCP 25番、POP3サーバー：TCP110番

- LAN(ホーム)側に別途ウェブサーバーを設置する場合は、そのサーバーのポート番号と本製品カメラモニター画面のポート番号(工場出荷時設定：80)と重ならないように設定する必要があります。オプション設定画面で本製品カメラモニター画面のポート番号の値を変更してください。(☞ 108ページ)
- 最大登録数は16個です。

設定例：
プライベートアドレスが192.168.0.2のパソコンにウェブサーバーを立ち上げてウェブサイトを公開する場合、TCPプロトコル、ポート番号：80(HTTPサービスポート番号)と192.168.0.2(プライベートアドレス)を入力します。
プライベートアドレスが192.168.0.3のパソコンにメールサーバーを立ち上げる場合、TCPプロトコル、ポート番号：25(メールサービスポート番号)と192.168.0.3(プライベートアドレス)を入力します。

設定例：

No.	操作	エントリー	対象接続	転送対象プロトコル	転送対象ポート	転送先IPアドレス
1	変更/削除	有効	*	TCP	80	192.168.0.2
2	変更/削除	有効	*	TCP	25	192.168.0.3

つづく

拡張機能を使う

「パソコンのIPアドレスを固定するには」（☞ 160ページ）を参考にTCP/IPの設定を行ってください。

静的IPマスカレードの転送先IPアドレスに設定した機器は、設定したプロトコル、ポートを通じてインターネットからアクセスすることができます。

データ入力欄

操作	各項目のパラメーターを変更／削除することができます。
エントリー	「有効」または「無効」を選びます。「有効」を選んだ場合、エントリーはテーブル(対象接続、プロトコル、転送対象ポート、転送先IPアドレス)に設定したように機能します。「無効」を選んだ場合、他の項目を設定しても機能しませんが、「有効」を選び直すと機能するようになります。
対象接続	1はメインセッション、2はサブセッションを表わします。“＊”を選ぶと、PPPoE全セッションおよびDHCP／Static接続が対象となります。
転送対象プロトコル	インターネットでデータを送受信する際に使うプロトコルを選びます。TCP、UDP、TCP&UDP、ESP、GRE、＊の中から選ぶことができます。ワイルドカード「＊」はすべてのプロトコルを意味します。
転送対象ポート	インターネットでデータを送受信する際に使うポートを指定します。 転送対象ポート範囲は0－65535の間で指定してください。 ポート番号は半角文字で入力し、スペースは入力しないでください。 ● ポートを1つだけ利用したいときは、そのポート番号を入力してください。 ● ポートの範囲を指定したい場合は、「－」を使って入力してください。例えば2000から3000までのポートを利用したい場合は、「2000－3000」と入力してください。小さいポート番号が左に、大きいポート番号が右になるように入力してください。
LAN側IPアドレス	本製品に接続されたパソコンのプライベートアドレスを設定します。インターネットからのデータは、このIPアドレスに送られます。対応するパソコンのIPアドレスをこの値に固定してください。

このテーブルを設定すると、インターネットから転送対象ポートへ不正アクセスされる可能性があります。安全のため、必要なときにのみ設定してください。

<追加のしかた>

1 アドレス変換画面の 端末型 をクリックする

静的IPマスカレード(ポートフォワーディング)

操作項目をクリックすると各設定画面が開き、変更/削除/追加ができます。

No.	操作	エントリー	対象接続	転送対象プロトコル	転送対象ポート	転送先IPアドレス
	追加					

2 静的IPマスカレード(ポートフォワーディング)で、操作項目の**追加**をクリックする

ポートフォワーディング設定画面が表示されます。

3 **設定の有効/無効、No.、対象接続、転送対象プロトコル、転送対象ポート、LAN側IPアドレス**、それぞれの項目を設定する

設定の有効/無効で「有効」をチェックすると、指定されたエントリーが使用中になります。「無効」をチェックするとそのエントリーは機能しませんが、次に必要になったときの設定を容易にするため、一度設定した設定内容は削除されずに残されます。

その他の項目については**データ入力欄**を参照してください。(☞ 84ページ)

4 追加 をクリックする

端末型画面に戻り、追加された情報欄がオレンジになります。

5 保存 をクリックする

設定が完了したことを知らせる再起動画面が表示されます。

6 再起動 をクリックする

拡張機能を使う

<変更／削除のしかた>

1 アドレス変換画面の 端末型 をクリックする

静的IPマスカレード(ポートフォワーディング)

操作項目をクリックすると各設定画面が開き、変更/削除/追加ができます。

No.	操作	エントリー	対象接続	転送対象プロトコル	転送対象ポート	転送先IPアドレス
1	変更/削除	**	***	***	***	***.***.***.***
	追加					

2 静的IPマスカレード(ポートフォワーディング)で変更または削除するNo.を選び、操作項目の**変更／削除**をクリックする

ポートフォワーディング設定画面が表示されます。

3 変更する場合には設定値を変更して 更新 を、削除する場合には 削除 をクリックする

端末型画面に戻ります。
変更された場合、情報欄がオレンジになり、変更後の設定値が表示されます。
削除された場合、情報欄がオレンジになり、「削除予定です」と表示されます。

4 保存 をクリックする

設定が完了したことを知らせる再起動画面が表示されます。

5 再起動 をクリックする

設定しました。

設定を完了するには再起動する必要があります。
後で再起動する場合は、再起動画面で再起動してください。
今すぐ再起動する場合は、再起動ボタンを押してください。

再起動

■ DMZ機能

DMZ(DeMilitarized Zone)機能を利用すると、WAN(インターネット)側からLAN(ホーム)側へ送られたあて先不明のパケットを、DMZで設定した特定のIPアドレスへ転送することができます。DMZによって転送されるパケットは、すべてのセキュリティフィルターを通過して、設定されたIPアドレスへ転送されます。

DMZ機能（端末型）

1 設定画面上の 端末型 をクリックする

2 エントリーのドロップダウンリストから「有効」を選び、DMZ機能のホストIPアドレス欄に、転送先IPアドレスを入力する

- 転送先に設定するIPアドレスは、LAN上にあるIPアドレスにしてください。
- 本製品のDMZ機能は、ポートフォワーディングによりLAN(ホーム)側に接続した機器のIPアドレスにデータを転送する機能です。転送先に設定したIPアドレスに対するフィルターは無効になります。本製品はセグメントを分けるDMZ機能ではないので、万一転送先に設定したIPアドレスが攻撃を受けた場合は、同じLAN(ホーム)側に接続しているほかの機器も攻撃される恐れがあります。セキュリティ面には十分に注意して、使用してください。
- DMZ機能を使用する場合は、アドレス変換を「使用する」に設定してください。(☞ 81ページ)
- カメラモニター(TCP80番[デフォルト])、設定画面(TCP8080番[デフォルト])およびPPTPサーバ機能(TCP1723番、GRE)についてはDMZ対象外です。また、IPv6接続でトンネル、6to4接続を設定している場合は、IPv6プロトコル（プロトコル番号41番）もDMZ対象外です。

3 設定を終えたら、保存 をクリックする

設定した内容が保存されます。

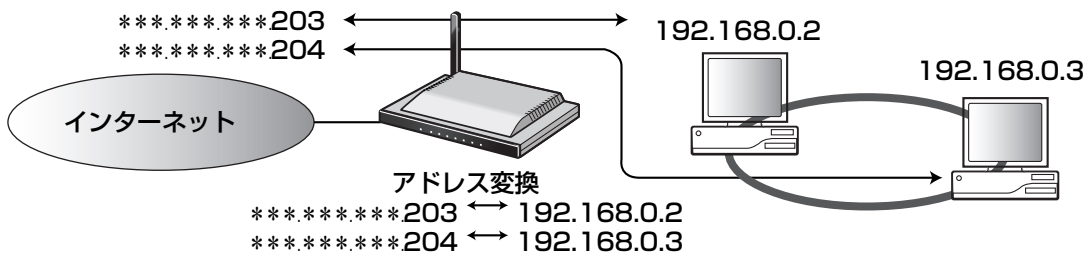
保存中は絶対に電源を切らないでください。保存中に電源を切ると本製品が正常に動作しなくなる可能性があります。

4 設定画面に、再起動 が表示されたら、それをクリックする

■ LAN型アドレス変換

プロバイダーから複数のグローバルアドレスを提供されているとき、グローバルアドレスとプライベートアドレスの相互変換の設定を行います。

静的NAT

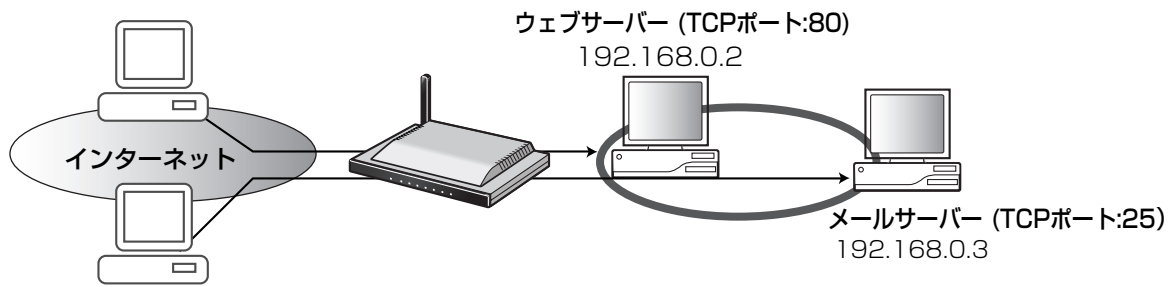
提供されているグローバルアドレスと、本製品に接続しているパソコンのプライベートアドレスを1対1で対応させます。

設定例：

グローバルアドレス***.***.***.203とプライベートアドレス192.168.0.2.を、***.***.***.204と192.168.0.3をそれぞれ1対1で対応させる場合は、次のように入力してください。必ず転送対象プロトコルに「*」を選んでください。転送対象ポート欄はマスクされます。入力後、転送対象ポート欄には「*」と表示されます。

No.	操作	エントリー	WAN側 IPアドレス	転送対象 プロトコル	転送対象 ポート	LAN側 IPアドレス
1	変更/削除	有効	***.***.***.203	*	*	192.168.0.2
2	変更/削除	有効	***.***.***.204	*	*	192.168.0.3
	追加					

つづく

静的IPマスカレード（ポートフォワーディング）

１つのグローバルアドレスを使って、WAN(インターネット)側のパソコンから、本製品に接続している複数のパソコンを参照することができます。

設定例：

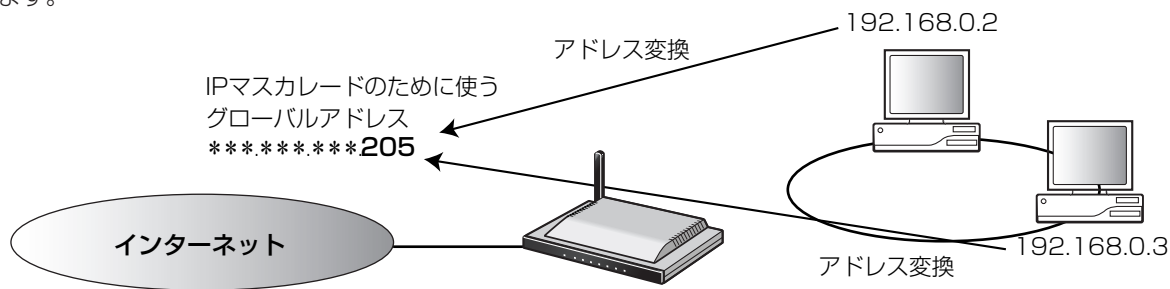
グローバルアドレス＊＊＊.＊＊＊.＊＊＊.203を通して、192.168.0.2や192.168.0.3のパソコンを参照させるには、次のように入力してください。

No.	操作	エントリー	WAN側 IPアドレス	転送対象 プロトコル	転送対象 ポート	LAN側 IPアドレス
1	変更/削除	有効	＊＊＊.＊＊＊.＊＊＊.203	TCP	80	192.168.0.2
2	変更/削除	有効	＊＊＊.＊＊＊.＊＊＊.203	TCP	25	192.168.0.3
	追加					

「パソコンのIPアドレスを固定するには」（☞ 160ページ）を参考にTCP/IPの設定を行ってください。

つづく

IPマスカレード

１つのグローバルアドレスを使って、複数のパソコンからインターネットに接続するときに、この機能を使います。

設定例：

No.	エントリー	IPマスカレード対象アドレス
1	有効	***.***.***.205

「無効」を選ぶと、本製品WAN側のIPアドレスが使用されます。

データ入力欄

エントリー	「有効」または、「無効」を選んでください。 「有効」を選んだ場合、設定されたIPマスカレード対象アドレスが使用されます。 「無効」を選んだ場合、設定されたIPマスカレード対象アドレスは使用されませんが、「有効」を選び直すと使用されるようになります。
IPマスカレード対象アドレス	インターネットでデータのやり取りをするグローバルアドレスを入力してください。

LAN型の設定で注意すること

- WAN(インターネット)側のIPアドレスが異なるとき、LAN(ホーム)側のIPアドレスを重複させることができません。
- LAN側IPアドレスの欄に、(プロバイダーから配布された)グローバルアドレスを入力しないでください。

No.	操作	エントリー	WAN側 IPアドレス	転送対象 プロトコル	転送対象 ポート	LAN側 IPアドレス
1	変更/削除	有効	***.***.***.202	TCP	10	192.168.0.2
2	変更/削除	有効	***.***.***.203	TCP	20	192.168.0.3
3	変更/削除	有効	***.***.***.204	TCP	30	192.168.0.4
	追加					

同一のアドレスを
入力しない

<追加のしかた>

1 アドレス変換画面の「LAN型」をクリックする

2 LAN型静的アドレス変換(静的NAT、静的IPマスカレード)で、操作の**追加**をクリックする

3 **設定の有効/無効、No.、WAN側IPアドレス、転送対象プロトコル、転送対象ポート、LAN側IPアドレス**、それぞれの項目を設定する

設定の有効/無効で「有効」をチェックすると、指定されたエントリーが使用中になります。「無効」をチェックするとそのエントリーは機能しませんが、次に必要になったときの設定を容易にするため、一度設定した設定内容は削除されずに残されます。

4 追加 をクリックする

LAN型画面に戻り、追加された情報欄がオレンジになります。

5 保存 をクリックする

設定が完了したことを知らせる再起動画面が表示されます。

6 再起動 をクリックする

<変更／削除のしかた>

1 アドレス変換画面の「LAN型」をクリックする

2 LAN型静的アドレス変換(静的NAT、静的IPマスカレード)で変更または削除するNo.を選び、操作項目の**変更／削除**をクリックする

アドレス変換画面が表示されます。

3 変更する場合には設定値を変更して 変更 を、削除する場合には 削除 をクリックする

LAN型画面に戻ります。
変更された場合、情報欄がオレンジになり、変更後の設定値が表示されます。
削除された場合、情報欄がオレンジになり、「削除予定です」と表示されます。

4 保存 をクリックする

設定が完了したことを知らせる再起動画面が表示されます。

5 再起動 をクリックする

DMZ機能(LAN型)

1 設定画面上の LAN型 をクリックする

2 エントリーのドロップダウンリストから「有効」を選び、グローバルアドレス欄にグローバルアドレス、ホストIPアドレス欄に転送先IPアドレスを入力する

最大4組を登録できます。

DMZ機能(LAN型)

No.	エントリー	グローバルアドレス	ホストIPアドレス
1	無効		
2	無効		
3	無効		
4	無効		

- 転送先に設定するIPアドレスは、LAN上にあるIPアドレスにしてください。
- 本製品のDMZ機能は、ポートフォワーディングによりLAN(ホーム)側に接続した機器のIPアドレスにデータを転送する機能です。転送先に設定したIPアドレスに対するフィルターは無効になります。本製品はセグメントを分けるDMZ機能ではないので、万一転送先に設定したIPアドレスが攻撃を受けた場合は、同じLAN(ホーム)側に接続しているほかの機器も攻撃される恐れがあります。セキュリティ面には十分に注意して、使用してください。
- DMZ機能を使用する場合は、アドレス変換を「使用する」に設定してください。(☞ 81ページ)
- 本製品WAN側に割り振られたIPアドレスのみカメラモニター(TCP80番[デフォルト])、設定画面(TCP8080番[デフォルト])およびPPTPサーバ機能(TCP1723番、GRE)についてはDMZ対象外です。また、IPv6接続でトンネル、6to4接続を設定している場合は、IPv6プロトコル（プロトコル番号41番）もDMZ対象外です。
- ホストIPアドレスの欄に、(プロバイダーから配布された)グローバルアドレスを入力しないでください。

3 設定を終えたら、 保存 をクリックする

設定した内容が保存されます。

保存中は絶対に電源を切らないでください。保存中に電源を切ると本製品が正常に動作しなくなる可能性があります。

4 設定画面に、 再起動 が表示されたら、それをクリックする

■ LAN型接続におけるグローバルアドレスとプライベートアドレスの混在

本製品では、LAN側にグローバルアドレス、プライベートアドレスの2つのネットワークアドレスをもつことが可能です。LAN側のパソコンにグローバルアドレスを割り振る方法は2種類あります。LAN型接続における本製品のグローバルアドレス(「本製品のIPアドレス」☞ 40ページ)は、LAN側のパソコンやカメラグローバルアドレスと重ならないアドレスを設定してください。

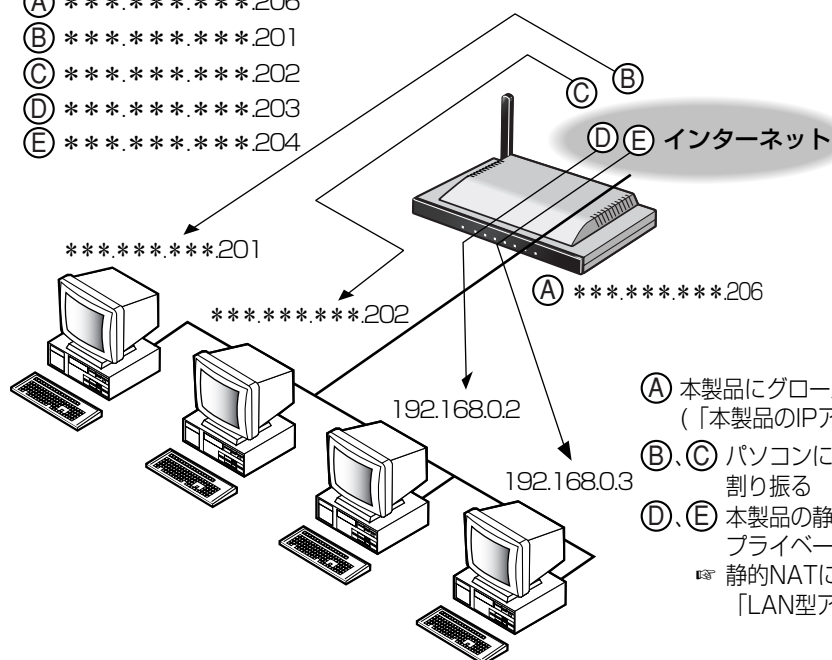
<静的NAT>

グローバルアドレスと、プライベートアドレスを1対1で変換します。

<グローバルアドレスをパソコンに直接設定>

プロバイダーから提供されたグローバルアドレスをLAN側パソコンに直接設定します。サブネットマスク、DNSサーバーはプロバイダーから指定されたものを設定してください。デフォルトゲートウェイはルーターに割り振るグローバルアドレス(「本製品のIPアドレス」☞ 40ページ)を指定してください。

(例)グローバルアドレスが以下の場合
Ⓐ ＊＊＊.＊＊＊.＊＊＊.206
Ⓑ ＊＊＊.＊＊＊.＊＊＊.201
Ⓒ ＊＊＊.＊＊＊.＊＊＊.202
Ⓓ ＊＊＊.＊＊＊.＊＊＊.203
Ⓔ ＊＊＊.＊＊＊.＊＊＊.204

Ⓑ Ⓒ
Ⓓ Ⓔ インターネット
＊＊＊.＊＊＊.＊＊＊.201
＊＊＊.＊＊＊.＊＊＊.202
Ⓐ ＊＊＊.＊＊＊.＊＊＊.206
192.168.0.2
192.168.0.3

Ⓐ 本製品にグローバルアドレスを割り振る
(「本製品のIPアドレス」☞ 40ページ)
Ⓑ、Ⓒ パソコンに直接グローバルアドレスを割り振る
Ⓓ、Ⓔ 本製品の静的NATを利用してパソコンにプライベートアドレスを割り振る
☞ 静的NATについては、88ページの「LAN型アドレス変換」を参照してください。

- 工場出荷時設定では、セキュリティ確保のため、グローバルアドレスをもつパソコンからプライベートアドレスをもつパソコンへはアクセスできない設定になっています。
  アクセス可能な状態に切り替えるには、 **セキュリティ設定** をクリックし、セキュリティワンタッチ設定画面で「G-IPからP-IPへの通信を禁止する。」のチェックをはずしてください。
- PPPoEマルチセッションを利用する場合、パソコンのDNSサーバーの設定は本製品のLAN側IPアドレスを設定して、DNSリレーを使用する必要があります。(☞ 110ページ)

IPv4接続でセキュリティを強化する

本製品へのアクセス制限およびフィルタリングの設定がワンタッチでできます。セキュリティ設定を行った場合、工場出荷時設定ではフィルタリングログが保存されます。保存されたログは、3文字の略語(☞ 次ページ)として画面に表示されます。

つづく

データ入力欄

● セキュリティワンタッチ設定	セキュリティ上重要で頻度の高いファイアウォールを、簡単に設定することができます。工場出荷時設定では、最もセキュリティが高くなるように設定しています。必要な場合のみ変更してください。
・「G-IPからP-IPへの通信を禁止する。」	ログ保存時の表示: G-P LAN型のPPPoE／Static接続において、LAN側にグローバルアドレス(G-IP)とプライベートアドレス(P-IP)が混在している場合、グローバルアドレスをもったパソコンからプライベートアドレスをもったパソコンへは通信を禁止します。工場出荷時設定では、「G-IPからP-IPへの通信を禁止する。」と「ログ出力」はチェックされています。
・「プライベートアドレスでのアクセスを双方向に禁止する。」	ログ保存時の表示：P-P WAN (インターネット) 側へ送信するパケットのあて先、またはWAN側から受信するパケットの送信元がプライベートアドレスの場合、本製品へのアクセスを禁止します。工場出荷時設定では、「プライベートアドレスでのアクセスを双方向に禁止する。」と「ログ出力」はチェックされています。
・「NetBIOS／ファイル共有／プリンター共有／PCリモートのアクセスは双方向に禁止する。」	ログ保存時の表示：SHR Windowsでファイルやプリンターを共有する際に送受信されるパケットの双方向アクセスを禁止しています。工場出荷時設定では、「NetBIOS/ファイル共有/プリンター共有/PCリモートのアクセスは双方向に禁止する。」と「ログ出力」はチェックされています。
● アクセス制限 ・設定画面	WAN側から本製品へのアクセス制限を設定します。 ログ保存時の表示: W-C WAN側から設定画面へのアクセスに対して、パスワードでの保護またはアクセスの禁止を選ぶことができます。工場出荷時設定では、「禁止する。」と「ログ出力」がチェックされています。
・カメラモニター画面	ログ保存時の表示: W-P WAN側からカメラモニター画面画面へのアクセスに対して、パスワードなしでの許可、パスワードでの保護、あるいはアクセスの禁止のいずれかを選ぶことができます。工場出荷時設定では、「パスワードなしで許可する。」と「ログ出力」がチェックされています。
● ステルスモードの設定 ・本製品の存在をWAN（インターネット）側ネットワークから検知できないようにする。	ログ保存時の表示：STL WAN (インターネット) 側から本製品の本体へのPingなどに応答しない設定をしています。応答しないため、Pingなどによる攻撃先の存在確認から逃れることができます。UDP/TCPポートスキャンにも応答しません。工場出荷時設定では、「本製品の存在をWAN(インターネット)側から検知できないようにする。」と「ログ出力」はチェックされています。
・Identパケットは例外とする。	ログ保存時の表示: STL(Ident) クライアント側がメールを送受信しようとするときに、クライアント側に対して認証を行うメールサーバーがあります。この認証はTCPの113番ポートを使った認証用の識別プロトコルを利用して行われます。この認証の重要度は低いので、メールの送受信ができなくなることは多くの場合ありません。工場出荷時設定では、「Identパケットは例外とする。」と「ログ出力」はチェックされています。

つづく

● 不正アクセス検知	不正アクセス検知機能を使用するときは、各項目のチェック欄をチェックしてください。
・ステートフル・パケット・インスペクション (動的パケットフィルタリング)を使用する。	ログ保存時の表示：SPI WAN側からの通信状態の予測に基づいて受信パケットを検査し、不正なパケットと判断された場合にはそのパケットを破棄します。静的なフィルタリング(ヘッダー情報でのパケット選別)と比較すると、より安全なインターネット通信ができます。工場出荷時設定では、「ステートフル・パケット・インスペクション(動的パケットフィルタリング)を使用する。」と「ログ出力」はチェックされています。
・攻撃検知をする。	ログ保存時の表示：DoS WAN 側からの悪意のある通信などを検知し、パケットを破棄します。またログへ検知記録を残します。 次のような攻撃を検知することができます。 ・TCPスキャン ・UDPスキャン ・ICMPエコー

各設定項目のログ出力のチェックをはずすと、ログが保存されません。

セキュリティを高めるためには、ソフトウェアなどの適切な運用およびバージョンアップが必要です。

<各セキュリティ機能の優先順位>

本製品はインターネット上のさまざまな不正アクセスに対応するために、以下のセキュリティ機能を装備しています。

【優先順位上位順】

・フィルタリング（☞ 98ページ）
・セキュリティワンタッチ設定（☞ 95ページ）
・ステルスモード（☞ 96ページ）

これらの機能は上から順に実行されます。条件に一致した時点でパケットの通過や破棄を決定します。

DMZ機能(☞ 87、93ページ)を利用している場合、DMZ端末に関係するパケットには、セキュリティ機能は実行されません。

拡張機能を使う

■ フィルタリング

IPアドレス、ポート、プロトコルの条件を指定することで、受信したIPパケットを通過、または遮断することができます。条件を適切に設定することで、セキュリティ対策として使用することができます。エントリーNo.の小さい順からフィルタリングの処理が行われます。フィルタリングの各項目の説明については、次ページを参照してください。

1 セキュリティ設定画面上の フィルタリング をクリックする

2 フィルタリング設定条件で、**追加**をクリックする

3 必要項目を設定し、 追加 をクリックする

4 設定を終えたら、 保存 をクリックする

設定した内容が保存されます。

5 設定画面に、 再起動 が表示されたら、それをクリックする

フィルタリング設定は、設定を終えたら必ず 保存 をクリックしてください。

つづく

データ入力欄

No.	エントリーNo. に1－64を選びます。エントリーNo. の小さい順にフィルタリングの処理を行います。すでに登録されている場合は、そのエントリーに上書きされます。
操作	新規でフィルタリングを設定するときは、「追加」をクリックしてください。このフィルタリング設定を変更、削除したい場合は、「変更／削除」をクリックします。設定画面が開き、フィルタリング設定の変更または、削除ができます。
エントリー	このフィルタリング設定が有効か、無効かを示します。
対象接続	1はメインセッション、2はサブセッションを表わします。“＊”を選ぶと、PPPoE全セッションおよびDHCP／Static接続が対象となります。
タイプ	許可(条件が一致すれば通す)、禁止(条件が一致すれば破棄する)のどちらかを選びます。
方向	W→L（WANからの受信時にフィルタリング）か L→W（WANへの送信時にフィルタリング）を選びます。
送信元IPアドレス／マスク長	フィルタリングするパケットの送信元IPアドレスを設定します。 ● IPアドレスを1つだけ指定したい場合は、IPアドレスとそのサブネットマスク長を入力してください。 ● IPアドレスの範囲を指定したい場合は、IPアドレス欄にネットワークアドレスを、マスク長欄にネットワークプレフィックス数を入力してください。例えば192.168.0.0／16のネットワークアドレスを指定したい場合は、IPアドレス欄に192.168.0.0、マスク長欄に16を入力します。 ● IPアドレスに＊を入力するとすべてのIPアドレスが対象になります。 （注）アドレス範囲を設定し、範囲の中に本製品のIPアドレスが含まれていても、本製品に対するフィルタリングは実行されません。本製品に対するフィルタリングが必要な場合は、IPアドレスに"＊"あるいは本製品をあらわす文字列（local）で入力する必要があります。
送信元ポート番号	フィルタリングするパケットの送信元ポート番号を設定します。 ● ポートを1つだけ利用したいときは、そのポート番号を入力してください。 ● ポートの範囲を指定したい場合は、「－」を使って入力してください。例えば2000から3000までのポートを利用したい場合は、「2000－3000」と入力してください。小さいポート番号が左に、大きいポート番号が右になるように入力してください。 ● ＊を入力するとすべてのポートが対象になります。
あて先IPアドレス／マスク長	フィルタリングするパケットのあて先のIPアドレスを設定します。入力の規則は送信元IPアドレスと同じです。 localを指定すると、本製品自身が対象となります。

つづく

あて先ポート番号	フィルタリングするパケットのあて先のポート番号を設定します。入力の規則は送信元ポートと同じです。
プロトコル	データを送受信する際のプロトコルを選びます。TCP、UDP、TCP&UDP、ICMP、ESP、GRE、＊の中から選びます。
ログ出力	パケット情報の記録を一時的に保存し、「フィルタリングログ」画面で表示する／しないを設定できます。

■ フィルタリングの項目を変更または削除するには

1. セキュリティ設定画面上の フィルタリング をクリックする
2. フィルタリング設定条件の一覧から、修正または削除する操作項目の**変更**／**削除**をクリックする
3. 設定項目を変更し、 更新 をクリックする
   削除するには 削除 をクリックする
4. 設定を終えたら、 保存 をクリックする
   設定した内容が保存されます。
5. 設定画面に、 再起動 が表示されたら、それをクリックする

■ フィルタリング項目の優先順位を変更するには

エントリーNo. の小さい順から、フィルタリングの処理を行います。フィルタリング項目の優先順位を変更するには、フィルタリング設定画面の「優先順位の変更」で、移動する項目のエントリーNo. を左の入力欄に入力し、移動先のエントリーNo. を右の入力欄に入力して、 移動 をクリックしてください。
そのあと、 保存 をクリックし、設定画面に 再起動 が表示されたら、それをクリックしてください。

IPv6接続でセキュリティを強化する

本製品へのIPv6接続でのアクセス制限、フィルタリングの設定がワンタッチでできます。セキュリティ設定を行った場合、工場出荷時設定ではフィルタリングログが保存されます。保存されたログは、3文字の略語（☞ 次ページ）として画面に表示されます。

IPv6セキュリティワンタッチ設定

- ☑ ダイレクトホスティングSMBのアクセスを双方向に禁止する。（☑ ログ出力）
- ☑ RPCに利用されるポートのアクセスを双方向に禁止する。（☑ ログ出力）
- ☑ 割り当てグローバルアドレス以外のグローバルアドレスを使った通信を禁止する。（☑ ログ出力）

IPv6ステルスモードの設定

- ☑ 本製品の存在をWAN(インターネット)側IPv6ネットワークから検知出来ないようにする。（☑ ログ出力）
  - ☑ Identパケットは例外とする。（☑ ログ出力）

IPv6不正アクセス検知

- ☑ IPv6ステートフル・パケット・インスペクション(動的パケットフィルタリング)（☑ ログ出力）
- ☐ IPv6による攻撃を検知する。（☑ ログ出力）

[保 存] [元に戻す]

つづく

データ入力欄

● IPv6セキュリティワンタッチ設定	セキュリティ上重要で頻度の高いファイアウォールを、簡単に設定することができます。工場出荷時設定では、最もセキュリティが高くなるように設定しています。必要な場合のみ変更してください。
・ダイレクトホスティングSMBのアクセスを双方向に禁止する。	ログ保存時の表示: SHR ダイレクトホスティングSMBのアクセスを双方向に禁止します。
・RPCに利用されるポートのアクセスを双方向に禁止する。	ログ保存時の表示：SHR RPCに利用されるポートのアクセスを双方向に禁止する。
・割り当てグローバルアドレス以外のグローバルアドレスを使った通信を禁止する。	ログ保存時の表示：GOR 割り当てグローバルアドレス以外のグローバルアドレスを使った通信を禁止します。割り当てグローバルアドレスとは、本製品WAN側IPv6アドレスとLAN側プレフィックス／プレフィックス長をもつIPv6アドレスのことです。
● IPv6ステルスモードの設定 ・本製品の存在をWAN（インターネット）側IPv6ネットワークから検知できないようにする。	ログ保存時の表示：STL WAN（インターネット）側から本製品の本体へのIPv6 Pingなどに応答しない設定をしています。応答しないため、IPv6 Pingなどによる攻撃先の存在確認から逃れることができます。UDP/TCPポートスキャンにも応答しません。工場出荷時設定では、「本製品の存在をWAN（インターネット）側から検知できないようにする。」と「ログ出力」はチェックされています。
・Identパケットは例外とする。	ログ保存時の表示: STL(Ident) クライアント側がメールを送受信しようとするときに、クライアント側に対して認証を行うメールサーバーがあります。この認証はTCPの113番ポートを使った認証用の識別プロトコルを利用して行われます。この認証の重要度は低いので、メールの送受信ができなくなることは多くの場合ありません。工場出荷時設定では、「Identパケットは例外とする。」と「ログ出力」はチェックされています。
● IPv6不正アクセス検知	不正アクセス検知機能を使用するときは、各項目のチェック欄をチェックしてください。
・IPv6ステートフル・パケット・インスペクション (動的パケットフィルタリング) を使用する。	ログ保存時の表示：SPI WAN 側からの通信状態の予測に基づいて受信パケットを検査し、不正なパケットと判断された場合にはそのパケットを破棄します。静的なフィルタリング(ヘッダー情報でのパケット選別)と比較すると、より安全なインターネット通信ができます。工場出荷時設定では、「IPv6ステートフル・パケット・インスペクション(動的パケットフィルタリング)を使用する。」と「ログ出力」はチェックされています。
・IPv6による攻撃を検知する。	ログ保存時の表示：DoS WAN側からの悪意のある通信などを検知し、パケットを破棄します。またログへ検知記録を残します。 次のような攻撃を検知することができます。 ・TCPスキャン ・UDPスキャン ・ICMPエコー

つづく

各設定項目のログ出力のチェックをはずすと、ログが保存されません。

セキュリティを高めるためには、ソフトウェアなどの適切な運用およびバージョンアップが必要です。

＜各セキュリティ機能の優先順位＞

本製品はインターネット上のさまざまな不正アクセスに対応するために、以下のセキュリティ機能を装備しています。

【優先順位上位順】

・IPv6フィルタリング（☞ 104ページ）
・IPv6セキュリティワンタッチ設定（☞ 101ページ）
・IPv6ステルスモード（☞ 102ページ）

これらの機能は上から順に実行されます。条件に一致した時点でパケットの通過や破棄を決定します。

■ IPv6フィルタリング

IPv6パケットのみをフィルタリングします。IPアドレス、ポート、プロトコルの条件を指定することで、受信したIPパケットを通過、または遮断することができます。条件を適切に設定することで、セキュリティ対策として使用することができます。エントリーNo.の小さい順からフィルタリングの処理が行われます。フィルタリングの各項目の説明については、次ページを参照してください。

1 セキュリティ設定画面上の IPv6フィルタリング をクリックする

2 フィルタリング設定条件で、**追加**をクリックする

3 必要項目を設定し、 追加 をクリックする

4 設定を終えたら、 保存 をクリックする

設定した内容が保存されます。

5 設定画面に、 再起動 が表示されたら、それをクリックする

フィルタリング設定は、設定を終えたら必ず 保存 をクリックしてください。

つづく

データ入力欄

No.	エントリーNo. に1－64を選びます。エントリーNo. の小さい順にフィルタリングの処理を行います。すでに登録されている場合は、そのエントリーに上書きされます。
操作	新規でフィルタリングを設定するときは、「追加」をクリックしてください。このフィルタリング設定を変更、削除したい場合は、「変更／削除」をクリックします。設定画面が開き、フィルタリング設定の変更または、削除ができます。
エントリー	このフィルタリング設定が有効か、無効かを示します。
方向	W→L（WANからの受信時にフィルタリング）か L→W（WANへの送信時にフィルタリング）を選びます。
送信元IPv6アドレス／ プレフィックス長	フィルタリングするパケットの送信元IPv6アドレスとポート番号を設定します。 ● IPv6アドレスを1つだけ設定するときは、プレフィックス長を128にしてください。例えば、2002:C0A8:1234:0123:4567:89ab:cdef:0123/128を設定する場合は、IPv6アドレスに2002:C0A8:1234:0123:4567:89ab:cdef:0123、プレフィックス長に128を入力します。 ● IPv6アドレスの範囲を設定するときは、通常プレフィックス長に64以下の値にしてください。例えば、2002:C0A8:1234::/48を設定する場合は、IPv6アドレスに2002:C0A8:1234::、プレフィックス長に48を入力します。 ● IPアドレスに＊を入力するとすべてのIPv6アドレスが対象になります。 （注）アドレス範囲を設定し、範囲の中に本製品のIPアドレスが含まれていても、本製品に対するフィルタリングは実行されません。本製品に対するフィルタリングが必要な場合は、IPアドレスに"＊"あるいは本製品をあらわす文字列（local）で入力する必要があります。
送信元ポート番号	フィルタリングするパケットの送信元ポート番号を設定します。 ● ポートを1つだけ利用したいときは、そのポート番号を入力してください。 ● ポートの範囲を指定したい場合は、「－」を使って入力してください。例えば2000から3000までのポートを利用したい場合は、「2000－3000」と入力してください。小さいポート番号が左に、大きいポート番号が右になるように入力してください。 ● ＊を入力するとすべてのポートが対象になります。
あて先IPアドレス／ プレフィックス長	フィルタリングするパケットのあて先のIPアドレスを設定します。入力の規則は送信元IPアドレスと同じです。localを指定すると、本製品が対象になります。
あて先ポート番号	フィルタリングするパケットのあて先のポート番号を設定します。入力の規則は送信元ポートと同じです。 （注）ポート番号53、80（カメラモニター画面）、1723、8080（設定画面）は使用されています。ほかのポート番号を設定してください。
プロトコル	データを送受信する際のプロトコルを選びます。TCP、UDP、TCP&UDP、ICMPv6、ESP、＊の中から選びます。ICMPv6は、タイプ番号を設定できます。 （注）ICMPv6を指定した場合、ICMPv6タイプ番号によっては、ネットワークに問題を生じることがあります。
ログ出力	パケット情報の記録を一時的に保存し、「フィルタリングログ」画面で表示する／しないを設定できます。

■ IPv6フィルタリングの項目を変更または削除するには

1 セキュリティ設定画面上の
[IPv6フィルタリング] をクリックする

2 フィルタリング設定条件の一覧から、修正または削除する操作項目の**変更**／**削除**をクリックする

3 設定項目を変更し、[更新] をクリックする
削除するには [削除] をクリックする

4 設定を終えたら、[保存] をクリックする
設定した内容が保存されます。

5 設定画面に、[再起動] が表示されたら、それをクリックする

■ IPv6フィルタリング項目の優先順位を変更するには

エントリーNo. の小さい順から、フィルタリングの処理を行います。フィルタリング項目の優先順位を変更するには、フィルタリング設定画面の「優先順位の変更」で、移動する項目のエントリーNo. を左の入力欄に入力し、移動先のエントリーNo. を右の入力欄に入力して、[移動] をクリックしてください。
そのあと、[保存] をクリックし、設定画面に [再起動] が表示されたら、それをクリックしてください。

IPv4接続でのオプション機能を使う

オプション設定画面では、LAN(ホーム)側の設定やWAN(インターネット)側にアクセスするための詳細な設定を行います。「IPアドレス(LAN側)DHCPサーバー」、「PPPoE」、「DNSリレー」、「MTUサイズ」、「ルーティング」、「UPnP」、「IPアドレス通知」の7項目について設定することができます。

オプション設定は、特に変更が必要な場合のみ行ってください。オプション設定を変更するには、次の手順に従ってください。

1 設定画面上の オプション設定 をクリックする

それぞれの入力欄については、次ページを参照してください。

2 画面の上にある設定項目を選ぶ

3 データ入力欄に設定値を入力する

元の設定に戻すには、元に戻す をクリックしてください。

4 設定を終えたら、保存 をクリックする

設定した内容が保存されます。

5 設定画面に、再起動 が表示されたら、それをクリックする

オプション設定を変更した場合、本製品に接続しているパソコンの設定を行い、パソコンを再起動してください。

■ IPアドレス(LAN側)DHCPサーバー

<LAN(ホーム)側IPアドレス設定>

LAN(ホーム)側IPアドレス設定	
IPアドレス(LAN側)	192.168.0.254
サブネットマスク	255.255.255.0
設定画面のポート番号	8080
カメラモニター画面のポート番号	80

IPアドレス（LAN側）	LAN(ホーム)側のIPアドレスを入力できます。工場出荷時設定は、192.168.0.254です。IPアドレスは、DHCP設定での「利用可能なアドレス範囲」、「VPN設定」での基本画面における「PPTPサーバーの設定」で指定されるPPTPサーバーの「利用可能なアドレス範囲」、「カメラ設定」でのカメラ登録画面における「カメラの自動登録機能の設定」で指定される「利用可能なアドレス範囲」と重複しないように設定してください。
サブネットマスク	LAN(ホーム)側のサブネットマスクを入力します。
設定画面のポート番号	設定画面のポート番号を入力します。65535までの範囲を使用してください。ただし、80を除く1－1023はウェルノウンポートのため、また、53、1723、10000は本製品が使用しているため、使用できません。
カメラモニター画面のポート番号	カメラモニター画面のポート番号を入力します。65535までの範囲を使用してください。ただし、80を除く1－1023はウェルノウンポートのため、また、53、1723、10000は本製品が使用しているため、使用できません。

<DHCPの設定>

DHCPの設定	
DHCPサーバー	◉ 使用する ○ 使用しない
利用可能なアドレス範囲	192.168.0.1 － 192.168.0.32

DHCPサーバー機能を使用することにより、LAN(ホーム)側に接続されている機器にIPアドレスを自動的に割り振ります。

DHCPサーバー	LAN(ホーム)側に接続されている機器にIPアドレスを自動的に割り振ります。工場出荷時設定は、「使用する」になっています。LAN(ホーム)側に接続されているすべての機器に手動でIPアドレスを設定する場合は、「使用しない」を選びます。DHCPサーバーの設定を変更した場合は、それぞれのパソコンのIPアドレスの設定を変更してください。
利用可能なアドレス範囲	DHCPサーバー機能を使用する際は、データ入力欄にプライベートアドレスの範囲を入力します。入力範囲は連続した最大128個の値です。特に必要ない限りは変更する必要はありません。

つづく

＜DHCPスタティック設定＞

DHCPサーバー機能を使うとき、パソコンのMACアドレスを登録することにより、パソコンに割り振るIPアドレスを固定することができます。

操作項目の**追加**をクリックすると、右の画面が表示されます。

設定の有効/無効 ◉有効 ○無効
IPアドレス(LAN側)
MACアドレス

設定の有効／無効	「有効」または「無効」を選んでください。「有効」を選んだ場合、エントリーテーブルは、テーブル設定したMACアドレスをもつパソコンを、テーブルで設定したIPアドレスに固定します。「無効」を選んだ場合、ほかの項目を設定しても機能しませんが、「有効」を選び直すと機能するようになります。
IPアドレス（LAN側）	該当するパソコンの固定したいIPアドレスを入力してください。
MACアドレス	該当するパソコンのLANカードのMACアドレスを入力してください。 必ず半角数字と半角英字の A ～ F またはa ～ f を2文字ずつ、半角の「:」で区切って“01:23:45:ab:cd:ef”のように入力してください。

■ PPPoE

PPPoEを利用してプロバイダーと接続する場合、PPPoEの接続を開始、または切断することができます。メインセッション、サブセッションの接続方法を選んでください。プロバイダーとの契約で、インターネットアクセスの利用料金が従量制の場合は、**「手動接続」**を選んでください。

「PPPoE」をクリックすると、右の画面が表示されます。

常時接続	電源が入っている間は常に接続されます。これが工場出荷時設定となっています。PPPoE接続／切断画面から手動で切断できます。 (☞ 133ページ)
手動接続	PPPoE接続は、PPPoE接続／切断画面で **接続** を選んだ場合にのみ接続されます（☞ 133ページ)。PPPoEの接続を切断するには、PPPoE接続画面上で **切断** をクリックしてください。

■ DNSリレー

LAN(ホーム)側に接続しているパソコンのIPアドレスを固定している場合などは、インターネットに接続するために、パソコンにDNSサーバーアドレスを入力する必要があります。DNSリレーはこの面倒な入力作業を省略します。DNSリレーにより本製品は、LAN(ホーム)側のパソコンに対して自身をDNSサーバーとして通知します。LAN(ホーム)側からのDNSの問い合わせに対しては、本製品がWAN(インターネット)側の指定のDNSサーバーに代理で問い合わせをします。そして、問い合わせで得た回答をLAN(ホーム)側のパソコンに返します。

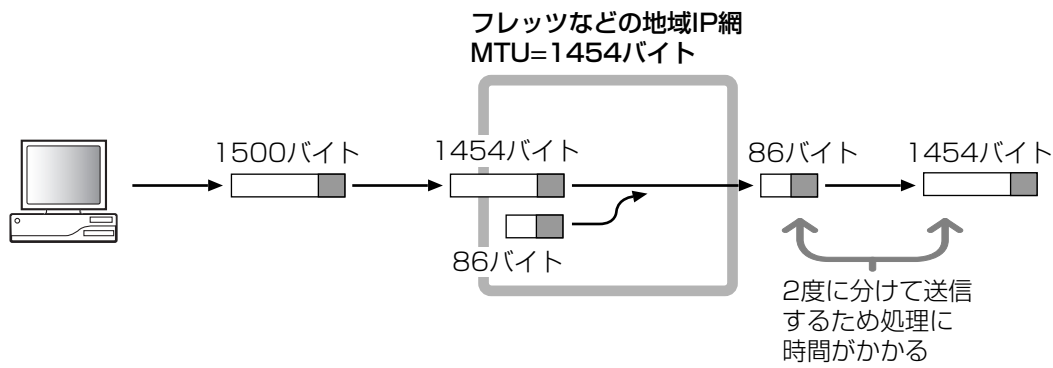
「DNSリレー」をクリックすると、設定画面が表示されます。

- PPPoEマルチセッションを利用する場合は、必ずDNSリレーを使用してください。
- LAN(ホーム)側にDNSサーバーを接続している場合は、DNSリレーを使用しないでください。

使用する	本製品をDNSサーバーの代理としてパソコンと通信します。 工場出荷時設定は「使用する」になっています。 パソコンのIPアドレスを固定している場合は、パソコンのDNSサーバーアドレス欄に本製品のIPアドレス192.168.0.254を入力します。
使用しない	DNSリレー機能が働きません。パソコンのIPアドレスを固定している場合は、パソコンのDNSサーバーアドレス欄にDNSサーバーのアドレスを入力します。

■ MTUサイズ

MTUとは、送信できるパケットの最大長をいいます。MTUの値が大きければ、１回に転送できる転送量が大きくなります。しかし、フレッツなどを使用するときに、MTUの値が大きすぎると、パケットが2回に分けられて送信されます。その結果、転送速度が低下します。通常は最適なMTU値になるように本製品が自動調整します。変更が必要な場合のみMTU値を変更してください。

「MTUサイズ」をクリックすると、設定画面が表示されます。

MTUの設定によっては、通信速度が極端に低下する場合があります。

■ ルーティング

ダイナミックルーティングとスタティックルーティングの設定を行うことができます。

「ルーティング」をクリックすると、設定画面が表示されます。

<ダイナミックルーティング設定>

LAN(ホーム)側設定	LAN(ホーム)側のRIP対応機器に対して、本製品が保持する経路情報を「送受信を行う／受信のみ／送信のみ／使用しない」に設定することができます。工場出荷時設定では「使用しない」になっています。
WAN(インターネット)側設定	経路情報をWAN(インターネット)側に送信すると、LAN(ホーム)側情報が外部から見えることになります。「送受信を行う／受信のみ／送信のみ／使用しない」のいずれかを選ぶことができます。工場出荷時設定では「使用しない」になっています。

つづく

拡張機能を使う

＜スタティックルーティング設定＞

本製品は、自動的に決定されるダイナミックルーティングのほかに、ゲートウェイを固定で4つまで設定することができます。これにより、本製品配下に複数のサブネットワークを構築したり、柔軟なルーティング設定を行うことができます。

1 オプション設定の「ルーティング」をクリックする

2 スタティックルーティング設定で、**エントリー**、**あて先IPアドレス**、**ネットマスク**、**ゲートウェイ**、**Metric**を設定する

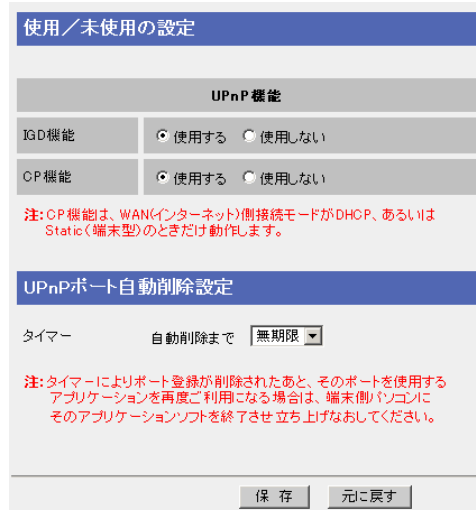
3 [保存] をクリックする

設定が完了したことを知らせる再起動画面が表示されます。

4 [再起動] をクリックする

データ入力欄

項目	説明
エントリー	この項目を「有効」に指定すると、入力されたスタティックルーティング設定が有効になります。スタティックルーティングを行わない場合は、「無効」にしておいてください。また「無効」に指定しても、次に必要となるときに設定しやすいように、入力されたほかの設定は削除されません。
あて先IPアドレス	あて先ホストまたはあて先ネットワークのIPアドレスを入力します。
ネットマスク	あて先IPアドレスに対するネットマスクを入力します。
ゲートウェイ	ゲートウェイのIPアドレスを入力します。
Metric	ドロップダウンリストから、Metric値を選びます。 Metricとは、パケットが通過するルーターの数を意味します。

スタティックルーティングで転送先に設定できるのは、本製品のネットワーク上にあるゲートウェイIPアドレスに限られます。ただし、DHCP、PPPoE接続でWAN側ポートに接続されたゲートウェイは、スタティックルーティングの転送先に設定することはできません。

■ UPnP™

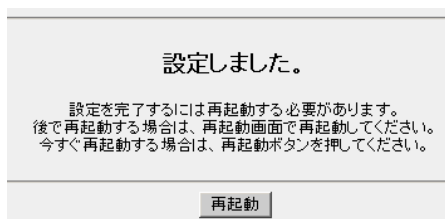
本製品はUPnP™に対応したアプリケーションやUPnP™対応機器を利用できます。UPnP™機能は、有線で接続したパソコン、無線で接続したパソコンのいずれからでも利用できます。UPnP™対応アプリケーション(Windows／MSN Messengerなど)の使いかたについては145ページを参照ください。

1 オプション設定の「UPnP」をクリックする

2 UPnP™機能を設定する

3 **「UPnPポート自動削除設定」**の時間を設定する

Messenger対応の機能により動的に開いたポートを削除するための時間を設定します。1～24時間の範囲で1時間単位で設定できます。“無期限”に設定するとポートの自動削除は行われません。この場合、ポートを削除するには本製品を再起動するか、ステータス内のUPnP™ポートマッピングテーブルを表示して **テーブル削除** をクリックし、手動で削除を行う必要があります。

- ポートが登録されてからは、上記で設定した時間が経過したら、強制的にポートが削除されます。アプリケーションの使用／未使用にかかわらず時間が経過すれば、ポートが閉じます。
- 音声チャットなどを24時間以上断続的に利用するときは、タイマー値を無期限にしてください。ポートを削除するには本製品を再起動するか、ステータス内のUPnP™ポートマッピングテーブルを表示して「テーブル削除」を実行し、手動で削除を行う必要があります。(☞ 138ページ)

4 設定を終えたら、 **保存** をクリックする

設定した内容が保存されます。

保存中は絶対に電源を切らないでください。保存中に電源を切ると本製品が正常に動作しなくなる可能性があります。

5 設定画面に、 **再起動** が表示されたら、それをクリックする

つづく

- アドレス変換の設定を変更した場合、本製品に接続しているパソコンの設定も行い、パソコンを再起動してください。
- UPnP™ポート自動削除設定の設定が無期限の場合、UPnP™で開いた外部ポートは、アプリケーションからの削除要求以外は閉じられません。セキュリティの面から、Windows／MSN Messengerを使用する場合は、自動削除するようにタイマーを設定してください。
  なお、Windows／MSN Messengerを起動している状態でタイマーによるポート削除によりリンクが切れた場合は、Windows／MSN Messengerをいったん終了してから起動し直してください。
  Windows／MSN Messengerをサインインし直すだけでは正常に動作しませんのでご注意ください。
- 本製品WAN側に接続されたUPnP™対応ルーターの配下で使用する場合、使用するルーター仕様によっては、本製品のセキュリティ設定によりIGD機能が動作しないことがあります。本製品のステルスモードの設定を無効にしてください。(☞ 95ページ)

UPnP™対応ルーターの配下で使用する

CP機能

CP機能を使用すると、本製品WAN側に接続されたUPnP™対応ルーター(以下、上位ルーターという)のポートマッピングを制御することができます。この機能をもつ機器をCP(コントロールポイント)と呼びます。この機能は本製品に登録されたカメラに対して有効です。

- 上位ルーターがUPnP™対応であっても、上位ルーターの仕様によっては、利用できないことがあります。
- 上位ルーターにWANからLANへの通信をフィルタリングする設定がなされている場合には、本製品のカメラモニター画面および本製品LAN側に接続されたカメラに対してインターネット側からアクセスできないことがあります。上位ルーターのフィルタリング設定の変更が必要です。
- 上位ルーターのウェブサーバーがポート番号80番を使用している場合、上位ルーターの設定を変更するか、本製品ウェブサーバーのポート番号を80番以外(例：8081番)に設定してください。
  (☞ 108ページ)
  本製品のウェブサーバーのポート番号を変えたときには、ウェブブラウザのアドレスバーにポート番号を指定してください。(例: http://WAN側IPアドレス:8081)
- 上位ルーターの仕様によっては、本製品のセキュリティ設定によりCP機能が動作しないことがあります。本製品のステルスモードの設定を無効にしてください。(☞ 95ページ)

UPnP™関連情報の表示

＜UPnP™ログ＞

Windows／MSN Messengerが本製品に対して行ったポートマッピングの状況について表示します。あらかじめオプション設定のUPnP™で、IGD機能を「使用する」に設定する必要があります。(☞ 113ページ)

Windows／MSN Messengerが本製品に対して行ったリクエストのログを、最新のものから表示します。最大ログ件数は400件です。400件を超えた場合は古いものから順に消去されます。また、本製品を再起動するとUPnP™ログ情報は消去されます。

UPnP™ログの確認方法については、139ページを参照してください。

■ IPアドレス通知

IPアドレス通知機能を使用することにより、WAN側IPアドレスを指定メールアドレスに通知することができます。これにより、WAN側に動的にIPアドレスが割り振られるサービス(DHCP、PPPoE接続)においてWAN側IPアドレスが変化した場合でもIPアドレスを知ることができるので、インターネットから本製品へアクセスすることができます。

IPアドレス通知内容

件名 (サブジェクト)	内容
ユーザー設定された文字列	WAN側のIPアドレス

受信メール例:

From: xxxxx@panasonic.com
Date: Mon, 07 Jun 2004 17:17:17 +0900
To: xxxxx@panasonic.com
Subject: IPアドレス通知
X-RCPT-TO: <yyyyy@zzz.co.jp>
111.222.333.444

- 設定情報を変更すると保存して再起動したあと、メール通知が行われます。
- PPPoE(マルチセッション)のときは、メインセッションのIPアドレスのみ通知します。サブセッションのIPアドレスは通知しません。
- SMTP認証には対応していません。

データ入力欄

IPアドレス通知	IPアドレス通知を「使用する」か「使用しない」にチェックを入れてください。「使用する」を選んだ場合、下記の項目を設定してください。
送信メール(SMTP)サーバー	送信メール(SMTP)サーバーのIPアドレスまたはホスト名を入力してください。
受信メール(POP3)サーバー	受信メール(POP3)サーバーのIPアドレスまたはホスト名を入力してください。
ログインID	受信メール(POP3)サーバーのログインIDを入力してください。
パスワード	受信メール(POP3)サーバーのパスワードを入力してください。
返信先（送信元）	返信先(送信元)のメールアドレスを入力してください。管理者のメールアドレスを入力することをおすすめします。
件名	件名を入力してください。
あて先1～5	Eメールの送信先のアドレスを5つまで設定できます。

IPv6接続でのオプション機能を使う

本製品のIPv6に関する詳細な設定を行います。工場設定値で不都合が生じた場合のみ設定を変更してください。通常、設定を変更する必要はありません。**IPv6に関して十分に理解したうえで、設定してください。**
オプション設定画面では、LAN（ホーム）側の設定やWAN（インターネット）側にアクセスするための詳細な設定を行います。「IPv6アドレス（LAN側）RA」、「リンクMTUサイズ」、「ルーティング」の3項目について設定することができます。

IPv6オプション設定は、特に変更が必要な場合のみ行ってください。IPv6オプション設定を変更するには、次の手順に従ってください。

1. 設定画面上の［IPv6オプション設定］をクリックする

   それぞれの入力欄については、次ページを参照してください。

2. 画面の上にある設定項目を選ぶ

3. データ入力欄に設定値を入力する

   元の設定に戻すには、［元に戻す］をクリックしてください。

4. 設定を終えたら、［保存］をクリックする

   設定した内容が保存されます。

5. 設定画面に、［再起動］が表示されたら、それをクリックする

IPv6オプション設定を変更した場合、本製品に接続しているパソコンの設定を行い、パソコンを再起動してください。

■ IPv6アドレス（LAN側）RA

LAN側のIPv6アドレス、RA（ルーター広告）の設定をします。
「IPv6アドレス（LAN側）　RA」をクリックすると、設定画面が表示されます。

＜LAN（ホーム）側IPv6アドレス設定＞

LAN(ホーム)側IPv6アドレス設定

IPv6アドレス(LAN側)　fe80:: 254

IPv6アドレス（LAN側）	本製品のLAN側IPv6リンクローカルアドレスの設定を行います。工場出荷時設定は、「fe80::254」です。

＜RA（LAN側IPv6自動設定）の設定＞

RA	本製品よりRA（ルータ広告）をLAN側に送信する、しないの設定を行います。特に不都合がなければ、設定を変更する必要はありません。工場出荷時設定は、「送信する」です。

RAは、WAN側にIPv6グローバルアドレスが付与されていない状態では、送信されません。

つづく

■ リンクMTUサイズ

WAN側のIPv6リンクMTUサイズを設定します。リンクMTUサイズとは、IPv6ネットワークセグメント内で送信できるIPv6最大パケットサイズのことです。MTUの値が大きければ、１回に転送できる転送量が大きくなります。

「リンクMTUサイズ」をクリックすると、設定画面が表示されます。

リンクMTUサイズ	IPv6リンクMTUサイズを1280～1500バイトの間で設定できます。特に不都合がなければ、設定を変更する必要はありません。工場出荷時設定は、「1500」です。

- リンクMTUの設定によっては、通信速度が極端に低下する場合があります。
- 接続形態によっては、設定した値が使われないことがあります。

■ ルーティング

ダイナミックルーティングとスタティックルーティングの設定を行うことができます。

「ルーティング」をクリックすると、設定画面が表示されます。

＜IPv6ダイナミックルーティング設定＞

LAN(ホーム)側設定	LAN(ホーム)側のRIPng対応機器に対して、本製品が保持する経路情報を「送受信する／受信のみ／送信のみ／使用しない」に設定することができます。工場出荷時設定では「使用しない」になっています。
WAN(インターネット)側設定	経路情報をWAN(インターネット)側に送信すると、LAN(ホーム)側情報が外部から見えることになります。「送受信する／受信のみ／送信のみ／使用しない」のいずれかを選ぶことができます。工場出荷時設定では「使用しない」になっています。

WAN側を「送受信する」または「送信する」にすると、WAN側へ本製品のLAN側ネットワーク情報が広告されるのでご注意ください。

つづく

<IPv6スタティックルーティング設定>

本製品は、自動的に決定されるダイナミックルーティングのほかに、ゲートウェイを固定で4つまで設定することができます。これにより、本製品配下に複数のサブネットワークを構築したり、柔軟なルーティング設定を行うことができます。

1 IPv6オプション設定の「ルーティング」をクリックする

2 スタティックルーティング設定で、**エントリー**、**あて先IPアドレス**、**ゲートウェイ**、**I/F**、**Metric**を設定する

3 保存 をクリックする

設定が完了したことを知らせる再起動画面が表示されます。

4 再起動 をクリックする

IPv6 スタティックルーティング設定

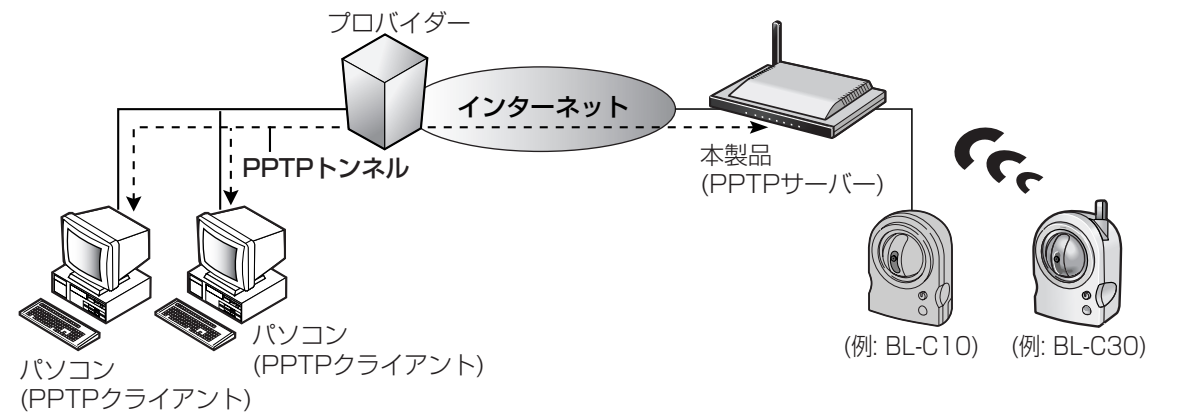
No.	エントリー	あて先IPv6アドレス ゲートウェイ	I/F	Metric
1	無効	/	LAN	
2	無効	/	LAN	
3	無効	/	LAN	
4	無効	/	LAN	

データ入力欄

エントリー	この項目を「有効」に指定すると、入力されたスタティックルーティング設定が有効になります。スタティックルーティングを行わない場合は、「無効」にしておいてください。また「無効」に指定しても、次に必要となるときに設定しやすいように、入力されたほかの設定は削除されません。
あて先IPv6アドレス	ルーティングするIPv6アドレスまたはプレフィックスを入力します。
ゲートウェイ	経路上にある本製品の次のルーターのIPv6アドレスを設定します。
I/F	ゲートウェイが存在するI/Fの設定をします。
Metric	あて先IPv6アドレスまでのホップ数を設定します。 1～255の間で指定できます。

VPN(PPTP)を使う

本製品は、PPTP(Point-to-Point Tunneling Protocol)によりVPN(Virtual Private Network: 私設仮想回線)を構築することができます。VPNとは、インターネットを介して専用線のように安全性を確保する仮想的な私設回線です。この機能を使って、遠隔地のパソコンからカメラ映像を安全に見ることができます。

パソコンのPPTP設定は154ページを参照してください。

1 PPTPサーバーを **「使用する」** にチェックを入れる

2 ユーザー名とパスワードを入力して 保存 をクリックする

ユーザー名とパスワードの設定完了を知らせる再起動画面が表示されます。

3 再起動 をクリックする

カメラコントロールユニットの再起動を知らせる画面のあと、トップページが表示されます。

PPTPサーバーの設定

PPTPサーバー　○使用する　◉使用しない

利用可能なアドレス範囲　192.168.0.100 - 192.168.0.101

注: 利用可能なアドレス範囲は最大2個です。

ユーザー登録

	ユーザー名	パスワード
1		
2		

データ入力欄

項目	説明
PPTPサーバー	「使用する」または「使用しない」を選んでください。
利用可能なアドレス範囲	接続時にPPTPサーバーからIPアドレスを割り振ります。利用可能なアドレス範囲は最大2個です。DHCPで使用されるIPアドレス(☞ 108ページ)と重複しないようご注意ください。工場出荷時設定は192.168.0.100－192.168.0.101です。
ユーザー名／パスワード	ユーザー名とパスワードを入力してください。2組まで登録できます。

つづく

本製品のPPTPサーバーと接続するPPTPクライアントは、Windows XPとWindows 2000のPPTPクライアントのみのサポートです。

■ 詳細

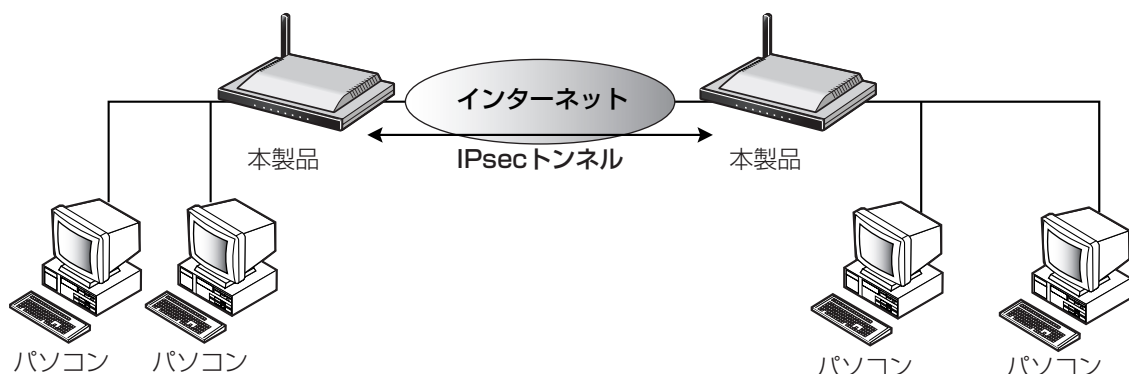
認証方式や暗号化方式の設定を行います。

1. 認証方式の設定で、「MS-CHAP、またはMS-CHAPv2を使用する」、または、「MS-CHAPv2のみ使用する」をチェックする
2. 暗号化方式の設定で、「なし、またはMPPE40bit、MPPE128 bitを許可する」、「MPPE40bitまたは、MPPE128 bitを許可する」、「MPPE128 bitを許可する」のいずれかをチェックする
3. 設定を終えたら、 保存 をクリックする
4. 設定画面に、 再起動 が表示されたら、それをクリックする

データ入力欄

認証方式の設定	パスワードの暗号化方式を指定します。MS-CHAPおよびMS-CHAPv2は、PPP接続時に、ユーザー名とパスワードを暗号化して相手認証を行う暗号化認証方式です。MS-CHAPは、クライアントから本製品への一方向の暗号化を行う認証方式です。これに対し、MS-CHAPv2は、クライアントと本製品の双方がそれぞれの身元を証明する相互認証方式などの機能が採用されていますので、MS-CHAPよりもセキュリティの点で向上しています。「MS-CHAP、またはMS-CHAPv2を使用する」または「 MS-CHAPv2のみ使用する」を選んでください。工場出荷時設定では「MS-CHAP、またはMS-CHAPv2を使用する」が選ばれています。
暗号化方式の設定	本文の暗号化方式を指定します。MPPEは、PPTPによるVPN接続のデータを暗号化します。MPPE128 bit(強力)およびMPPE40 bit(標準)の2つの暗号化方式があり、PPTP接続と本製品の間のデータセキュリティを強化します。「なし、またはMPPE40 bit、MPPE128 bitを許可する」、「MPPE40 bitまたは、MPPE128 bitを許可する」、「 MPPE128 bitを許可する」のいずれかを選んでください。工場出荷時設定では「MPPE40 bitまたは、MPPE128 bitを許可する」が選ばれています。

VPN（IPsec）を使う

本製品のIPv6通信では、IPsecでVPNを構築することができます。VPNとは、インターネットを介して専用線のように安全性を確保する仮想的な私設回線です。**この機能は、IPv6やVPNに関して十分に理解したうえで、設定してください。**

1 IPsecを **「使用する」** にチェックを入れる

本製品は、イニシエータ、レスポンダーのどちらでも動作します。

2 セキュリティポリシー・データベースの **追加** をクリックする

接続先情報設定画面が表示されます。
最大2個まで登録できます。

3 必要な項目を設定し、［**追加**］をクリックする

カメラコントロールユニットの再起動を知らせる画面のあと、トップページが表示されます。

接続先情報

データベース名	
エントリー	◉有効 ○無効
事前共有鍵	
事前共有鍵の再入力	
	(※)半角英数字8～64で入力可能です。
接続相手のWAN側IPv6アドレス	
接続相手のLANネットワーク	/
詳細な設定	詳細編集

追 加　元に戻す　キャンセル

4 ［**保存**］をクリックする

5 ［**再起動**］をクリックする

つづく

■ セキュリティポリシー・データベース

セキュリティポリシー・データベースのエントリーは、最大2個まで登録できます。

データ入力欄

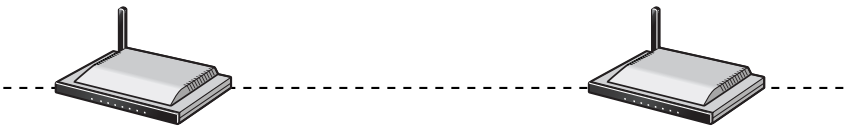
データベース名	IPsec通信を行うデータベースの名称を入力します。
エントリー	「有効」に指定すると、入力されたIPsec設定が有効になります。IPsecを行わない場合は、「無効」にしておいてください。また「無効」に設定しても、入力されたほかの設定は削除されません。
事前共有鍵	事前共有鍵を設定します。半角英数で8〜64文字で入力してください。この事前共有鍵を基に、IPsecで使用される秘密共有鍵が生成されるため、事前共有鍵は、第三者に知られないように注意をしてください。通信の安全性が保たれなくなります。
接続相手のWAN側IPv6アドレス	接続相手のWAN側IPv6グローバルアドレスを設定します。
接続相手のLANネットワーク	接続相手のLANネットワークのプレフィックスとプレフィックス長を設定します。プレフィックスは、グローバルなプレフィックスを設定してください。また、本製品のLAN側ネットワークは、接続相手のLANネットワークとは別のネットワークにしてください。また、リンクローカルアドレスを設定することはできないのでご注意ください。
詳細な設定	IPsecに関するさらに詳細な設定を行うことができます。(☞ 125ページ)

● WAN側IPv6アドレス、接続相手のLANネットワーク入力例

IPsec接続例（1）

接続相手のWAN側IPv6アドレス
2001:1002::＊＊＊＊

自装置のLANネットワーク1:
2001:1001:＊＊＊＊::/64

接続相手のLANネットワーク2:
2001:1002:＊＊＊＊::/64

接続相手のWAN側IPv6アドレスとして、"2001:1002: :＊＊＊＊"を入力します。
接続相手のLANネットワークとして、"2001:1002:＊＊＊＊::"、プレフィックス長"64"を入力します。

つづく

IPsec接続例（2）
以下のような形態の場合、LANネットワーク1とLANネットワーク2が同じネットワークになっているので、IPsecで通信できません。

接続相手のWAN側IPv6アドレス
2001:1002::∗∗∗∗

自装置のLANネットワーク1:
2001:1001:∗∗∗∗::/64

接続相手のLANネットワーク2:
2001:1001:∗∗∗∗::/64

接続相手のLANネットワークのプレフィックス長について
接続相手が本製品の場合、設定するプレフィックス長は以下のようになります。
- トンネル、Static V6接続：LAN側プレフィックスで設定したプレフィックス長を設定する。
- 6to4接続：48に設定する。
- PPPoE IPv4/IPv6接続：接続相手が加入しているIPv6対応プロバイダーが配布するプレフィックス長を設定する。

■ IPsec詳細設定

IPsec接続の詳細な設定を行うことができます。通常は、設定を変更する必要はありません。IPsecに関して十分に理解したうえで、設定してください。

つづく

＜基本設定＞

項目	説明
ID	自分の身元を示すIDを設定します。「IPv6アドレス」と「ドメイン名」を設定できます。ドメイン名を設定したときは、必ず交換モードを「アグレッシブ」に設定してください。
ドメイン名	IDがドメイン名のとき、ドメイン名を設定します。
自装置のLAN側IPv6アドレス	パケットの送信元IPアドレスを「すべて」または「指定する」に設定します。「すべて」に設定すると、本製品のLAN側にあるすべてのグローバルアドレスを対象にして、IPsecでパケットのカプセル化を行います。「指定する」にすると、本製品のLAN側ネットワークアドレスで指定されたグローバルアドレスを対象にして、IPsecでカプセル化を行います。
自装置のLAN側ネットワーク	「自装置のLAN側IPv6アドレス」が「指定する」に設定されたときの本製品LAN側のパケット送信元ネットワークアドレス（プレフィックス）を設定します。

＜フェーズ1の設定＞

項目	説明
交換モード	IKE フェーズ1の交換モードを「メイン」または「アグレッシブ」から設定します。「アグレッシブ」は、鍵交換は「メイン」に比べると簡略ですが、セキュリティはやや弱くなります。
ライフタイム	IKE SAのライフタイムを設定します。5分～2400時間の間で設定できます。
プロポーザル・エントリ	このプロポーザルの「有効」、「無効」を設定します。「無効」に設定された項目は、プロポーザルされません。
プロポーザル・暗号化方式	フェーズ1で使用される暗号化方式を設定します。暗号化方式は、「DES」、「3DES 」、「AES（128 bit)」、「AES (192 bit)」、「AES (256 bit)」から選ぶことができます。
プロポーザル・ハッシュ	フェーズ1で使用される認証アルゴリズム（ハッシュ）を設定します。「MD5」と「SHA-1」から選ぶことができます。
プロポーザル・DHグループ	フェーズ1で使用するDH（Diffie-Hellman）グループを設定します。DHグループとは、Diffie-Hellman公開値のことで、DHグループは、「1」と「2」から選ぶことができます。DHグループは、「1」に比べ「2」の方が、セキュリティが強固ですが、「1」でも脆弱ではありません。 交換モードを「アグレッシブ」にしたときは、DHグループに「1」と「2」を混在させないでください。

つづく

＜フェーズ2の設定＞

ライフタイム	IPsec SAのライフタイムを設定します。5分〜2400時間の間で設定できます。
PFS	フェーズ2でPFS（Perfect Forward Security）をする、しないを設定します。「有効　DHグループ2」、「有効　DHグループ1」、「無効」から選ぶことができます。「有効　DHグループ2」は、フェーズ2で再度Diffie-Hellman交換を行い、DHグループ2による秘密共有鍵を生成します。「有効　DHグループ1」は、フェーズ2で再度Diffie-Hellman交換を行い、DHグループ1による秘密共有鍵を生成します。「無効」は、フェーズ2でも、フェーズ1で生成した秘密共有鍵を使用します。PFSを「有効」とした方が、「無効」とした場合より、セキュリティが強くなります。
プロポーザル・エントリ	プロポーザルの「有効」、「無効」の設定を行います。「無効」に設定された項目は、プロポーザルされません。
プロポーザル・暗号化方式	暗号化方式を設定します。暗号化方式は、「DES」、「3DES 」、「AES（128 bit)」、「AES（192 bit)」、「AES（256 bit)」、「NULL」から選ぶことができます。
プロポーザル・ハッシュ	認証アルゴリズム（ハッシュ）を設定します。「MD5」と「SHA-1」、「なし」から選ぶことができます。

管理する

パスワードを変更する

設定画面およびカメラモニター画面へアクセスするためのパスワードを変更します。

1 設定画面上の パスワード設定 をクリックする

2 設定画面またはカメラモニター画面のユーザー名入力欄に新しいユーザー名を6～15文字までの半角英数字で入力する

3 パスワード入力欄に新しいパスワードを6～15文字までの半角英数字で入力し、確認のため、パスワードの再入力欄に再度新しいパスワードを入力する

- パスワードの再入力欄に入力する際は、コピー・貼り付け機能を使わないでください。
- 大文字、小文字を区別してユーザー名とパスワードを入力してください。

4 保存 をクリックする

- パスワードの変更が終了したら、右の画面が表示されます。

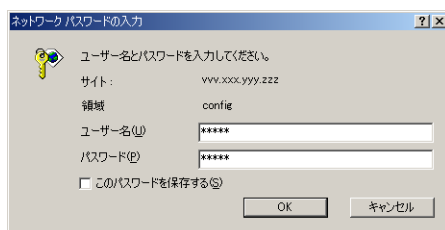
設定しました。

設定を完了するには再起動する必要があります。
後で再起動する場合は、再起動画面で再起動してください。
今すぐ再起動する場合は、再起動ボタンを押してください。

再起動

- 入力されたパスワードがまちがっていると、右の画面が表示されます。

つづく

5 **ネットワークパスワードの入力**ダイアログボックスが表示されたら、**ユーザー名**と**パスワード**欄に新しいユーザー名とパスワードを入力し、 OK をクリックする

設定したユーザー名とパスワードを忘れてしまった場合
CLEAR SETTINGボタンを押して本製品の初期化を行ってください。(☞ 144ページ)
設定内容が工場出荷時の状態に戻ります。もう一度ユーザー名とパスワードを設定し直してください。

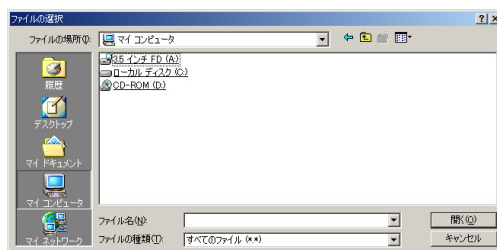
バージョンアップする

お客さまプライバシー情報の漏えい、本製品の不正操作、妨害や停止などを防ぐために、最新のファームウェアを入手してバージョンアップを行ってください。最新ファームウェアファイルは、パナソニックのサポートウェブサイト(http://panasonic.co.jp/pcc/products/hnetwk/support/) から入手することができます。

バージョンアップ機能を使う前に、パソコンにファームウェアファイルをダウンロードしてください。
詳細は、サポートウェブサイトの説明をお読みください。
古いバージョンのファームウェアをダウンロードするときには、設定情報が初期化されることがあります。詳細は、リリースノートを参照ください。

1 設定画面上の バージョンアップ をクリックする

2 ファームウェアファイルを選ぶために、 参照... をクリックする

ファイルの選択ダイアログボックスが表示されます。

3 ファイルの一覧からインストールしたいファームウェアファイルを選び、 開く をクリックする

選んだファイルがバージョンアップ画面の**ファイル名**欄に表示されます。

つづく

4 開始 をクリックする

バージョンアップを行います。

バージョンアップ中は絶対に電源を切らないでください。更新中に電源を切ると正常に動作しなくなります。
(バージョンアップ中に誤って電源を切ってしまった場合は、次に電源を入れたときにPOWERインジケーターが緑点滅しますので、「ご使用の前に／困った時には」の15ページにある「POWERインジケーターが緑に点滅する」を参照して、再度ファームウェアのバージョンアップを行ってください。)

- バージョンアップが終了すると、自動的に再起動します。
- バージョンアップされなかったときは、エラーメッセージが表示されます。
（下記表を参照してください。）

- バージョンアップ後、初期化を必要とする場合があります。詳細はパナソニックのサポートウェブサイトを参照してください。初期化はCLEAR SETTINGボタン(☞ 144ページ)を押してください。
- DHCPサーバー機能(☞ 108ページ)を使っているときは、本製品に接続しているLAN(ホーム)側のすべてのパソコンを再起動してください。

エラーメッセージ	原因と対策
正しいファイルではありません。	選んだファームウェアファイルは、本製品には使えません。適切なファイルを選んでください。ファイルに添付されている説明書（Readme.txtなど）を参照して、本製品のハードウェアバージョンに合っているか確認してください。(☞ 136ページ）合っていないときは、ハードウェアバージョンに合う最新版のファームウェアファイルをhttp://panasonic.co.jp/pcc/products/hnetwk/support/より入手してください。
メモリーが足りません。	本製品の内蔵メモリーが処理負荷のため少なくなっています。 本製品を再起動したあと、再度バージョンアップを行ってください。

バックアップする

各種設定ファイルのバックアップと、バックアップしたファイルの復元ができます。

■ 設定ファイル作成

設定ファイルバックアップ

バックアップファイルの作成

1 設定画面上の［バックアップ］をクリックする

2 「バックアップファイルの作成」をクリックする

ダウンロードのウィザード画面が表示されます。

3 保存する場所とファイル名を指定して保存する

■ 設定ファイル復元

1 設定画面上の［バックアップ］をクリックする

2 **復元させるファイルを選ぶために、［参照...］をクリックする**

ファイルの選択ダイアログボックスが表示されます。

3 ファイルの一覧から復元させるバックアップファイルを選び、［開く］をクリックする

選んだファイルが設定ファイル復元設定画面のファイル名欄に表示されます。

4 ［復元］をクリックする

5 ［再起動］をクリックする

再起動されます。

復元しようとする設定ファイルが壊れていたり間違っている場合は、エラー画面が表示されます。詳細は実際の画面を参照ください。

再起動する

再起動します。このとき、本製品の設定内容は保存されています。

1 設定画面上の 再起動 をクリックする

再起動します

再起動

2 再起動 をクリックする

再起動されます。

DHCPサーバー機能(☞ 108ページ)を使っているときは、本製品に接続しているLAN(ホーム)側のすべてのパソコンも再起動してください。

初期化する

すべての設定値を初期化します。設定値は、工場出荷時に設定されていた内容(工場出荷時設定 ☞ 131ページ)に戻ります。

1 設定画面上の 初期化 をクリックする

現在の設定を初期化します

初期化

2 初期化 をクリックする

すべての設定値が初期化されます。

DHCPサーバー機能(☞ 108ページ)を使っているときは、本製品に接続しているLAN(ホーム)側のすべてのパソコンも再起動してください。

PPPoE接続 ／切断を使う

PPPoEの接続コマンドによって、プロバイダーへのPPPoE接続を手動で切断または接続することができます。本製品の電源を切るときは、PPPoE接続を手動で切断したあとに電源を切ってください。PPPoE接続を手動で切断する前に本製品の電源を切ると、再接続時に時間がかかる場合があります。

<PPPoE接続を行う場合>

1. 設定画面上の PPPoE接続／切断 をクリックする
2. PPPoE接続を開始するには、各セッションの 接続 をクリックする

<PPPoE接続を切断する場合>

1. 設定画面上の PPPoE接続／切断 をクリックする
2. 接続を切断するには、各セッションの 切断 をクリックする

- このコマンドは、PPPoEの接続形態の種類(常時接続または手動接続)に関係なく使用できます。
- WAN(インターネット)側からは、PPPoEの切断はできません。

セッション・キープ・アライブ機能について

本製品はセッション・キープ・アライブ機能をもっています。PPPoE接続の常時接続モードの場合に、プロバイダーのサーバーとの接続が何らかの理由で切断したときに、自動的に接続を試みる機能です。本製品のセッション・キープ・アライブ機能は次の特徴をもっています。

- 常時接続モード時に有効になっています。手動接続モード時は、自動的に接続しません。
- 再接続を行うタイミングは、1分後、2分後、3分後…9分後と1分ずつ増えていき、それ以降は10分間隔で接続を試みます。

VPN（IPsec）接続 ／切断を使う

VPN（IPsec）接続を手動で切断または接続することができます。

<VPN（IPsec）接続を行う場合>

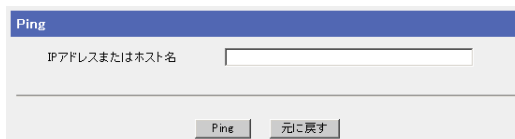
1. 設定画面上の VPN（IPsec）接続／切断 をクリックする
2. VPN（IPsec）接続を開始するには、各セッションの 接続 をクリックする

<VPN（IPsec）接続を切断する場合>

1. 設定画面上の VPN（IPsec）接続／切断 をクリックする
2. 接続を切断するには、各セッションの 切断 をクリックする

ネットワークの接続を確認する

WAN(インターネット)側、または、LAN(ホーム)側のウェブサイトや機器が、TCP/IPネットワークで本製品と接続されているかどうか、確認することができます。正しく接続されている場合は、「成功！」のメッセージが画面に表示されます。

1 設定画面上の [Ping] をクリックする

2 接続されていることを確認したい機器やサイトのIPアドレス(例：192.168.0.1)またはホスト名(例: panasonic.jp)を入力する

IPアドレスまたはホスト名欄を空白に戻すには、[元に戻す] をクリックする

3 [Ping] をクリックする

- 接続されている場合は、右の画面が表示されます。
- 指定IPアドレスからの応答がない場合は、右の画面が表示されます。

- Pingを実行したウェブサイトが接続されていても、ウェブサイトによってはPingに応答しない場合があります。この場合、「失敗」と表示されます。
- ホスト名がDNSで解決できない場合にも、「見つかりません」というエラー画面が表示されます。
- IPv6アドレスを入力することはできません。

情報を知る

ネットワーク情報を知る

お客様ご相談センターに連絡するときに役に立ちます。「ネットワーク接続情報」と「UPnPポートマッピングテーブル」、「カメラ登録情報」によって、本製品のネットワーク接続に関する諸情報を表示します。

■ ネットワーク接続情報

ハードウェアとソフトウェアのバージョン情報などを見ることができます。この情報は、お客様ご相談センターに連絡するとき役に立ちます。

1 設定画面上の ステータス をクリックする

IPv6接続を行っているときは、IPv6ネットワーク情報が表示されます。

2 ネットワーク接続情報の 表示 をクリックする

IPv6ネットワーク情報を表示するときは、IPv6ネットワーク情報の 表示 をクリックする

表示画面最下部のステータス保存をクリックすると、ファイルのダウンロード画面が表示されます。保存する場所とファイル名を指定して表示内容を保存できます。

■ UPnP™ポートマッピングテーブル表示

本製品に登録したUPnP™ポートマッピング設定情報が表示されます。最大128件まで表示されます。また、本製品を再起動するとUPnP™ポートマッピング登録情報は消去されます。
UPnP™ポートマッピング設定情報は次の手順で確認することができます。

1 設定画面上の ステータス をクリックする

2 ステータス下部の「UPnPポートマッピングテーブル」の 表示 をクリックする

No.	状態	クライアント	プロトコル	外部ポート	内部ポート	リモートホスト	有効期間（秒）	登録日時	説明
1	有効	192.168.0.1	TCP	80	80	*	1080	10/08 13:09:58	CamPortMapping

つづく

情報を知る

■ 表示項目

登録されたUPnP™ポートマッピングの設定情報

項目	内容
登録件数	UPnP™ポートマッピングの最大登録数は128件です。 以下、2つの状態を示します。 1 「アドレス変換」で「使用する（UPnP対応）」を選んでいる場合、「登録件数：現在の登録件数／128」が表示されます。 2 「アドレス変換」で「使用する（UPnP対応）」を選んでいない場合、「登録件数：0／128」が表示されます。
UPnP™ポートが登録されてから、自動削除されるまでの時間	アドレス変換設定で登録したUPnP™ポート自動削除設定の値（無期限、1～24時間）が表示されます。 注：登録日時から設定時間が経過すると、ポートが自動削除されます。
状態	ポートマッピングの設定が有効か無効かが表示されます。
クライアント	クライアントのIPアドレスが表示されます。
プロトコル	設定された情報の対象となるプロトコルが表示されます。「TCP」または「UDP」が表示されます。
外部ポート	設定されたポート情報の外側（WAN側）のポート番号が表示されます。
内部ポート	設定されたポート情報のクライアント側のIPアドレスとポート番号が表示されます。
リモートホスト	クライアントから通信相手を特定してポート追加要求された場合、相手のホストIPアドレスが表示されます。通信相手に制限がなければ、＊が表示されます。
有効期限（秒）	クライアントから登録UPnP™ポートに対して有効期限が設定される場合は、その有効期限が秒で表示されます。有効期限が設定されない場合は無期限と表示されます。
登録日時	クライアントがUPnP™で登録アクセスしてきた日時が表示されます。 注：この時間は表示しているパソコンの現在時刻を基に算出しています。表示されている日時がおかしい場合は、パソコンの時刻設定を確認、調整してください。
説明	アプリケーションから送られてくる情報が表示されます。

つづく

<UPnP^{TM}ポートマッピングテーブル登録情報消去>

本製品に登録したUPnP^{TM}ポートマッピングテーブルを強制的に消去することができます。テーブル削除ボタンを押すと、すべてのUPnP^{TM}ポートマッピングテーブルが消去されます。

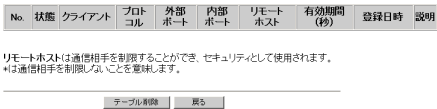
UPnP^{TM}ポートマッピングテーブル登録の全消去は次の手順で行います。

1 UPnP^{TM}ポートマッピングテーブル画面で テーブル削除 をクリックする

テーブルが全削除された画面が表示されます。

No.	状態	クライアント	プロトコル	外部ポート	内部ポート	リモートホスト	有効期間(秒)	登録日時	説明

リモートホストは通信相手を制限することができ、セキュリティとして使用されます。
*は通信相手を制限しないことを意味します。

テーブル削除　戻る

- Windows／MSN Messengerを終了してもUPnP^{TM}ポートマッピングが残ることがあります。それによりUPnP^{TM}ポートマッピング最大登録件数128件を越える登録がされた場合、その登録は無視され､正常にWindows／MSN Messengerが利用できなくなることがあります。その場合は、ポートマッピングテーブルを一度削除してください。
- Windows／MSN Messengerを起動している状態でUPnP^{TM}ポートマッピング登録情報を消去して接続が切れた場合は、Windows／MSN Messengerをいったん終了後、起動し直してください。Windows／MSN Messengerをサインインし直すだけでは正常に動作しませんので注意してください。

■ カメラ登録情報表示

本製品に登録したカメラの登録情報が表示されます。最大16件まで表示されます。自動設定を行ったカメラが対象となります。手動で設定を行ったカメラの情報は表示されません。カメラ登録情報は次の手順で確認することができます。

1 設定画面上の ステータス をクリックする

2 ステータス下部の「カメラ登録情報」の 表示 をクリックする

登録件数：　1/ 16

No.	カメラ名	状態
1	cam1	非公開

戻る

各種ログを知る

本製品が取得している各種ログを表示します。最新のログから順に表示され、ログ満杯時には、古いログから削除されて新しいログが上書きされていきます。

- 本製品の設定には、最低限、ユーザー名／パスワードによる認証を常に行ってください。
- 本製品へアクセスするためのユーザー名／パスワード、本製品に対する設定情報、アプリケーション設定情報、ログなどのシステム管理情報は、お客様の責任管理下にあります。それらの情報に関わる利用者または利用者グループ以外の第三者が、参照、更新、削除、複写できないようにアクセス制限をしたり、利用者以外にはユーザー名／パスワードやその他の設定・管理情報は秘密にしてください。
- ログ日時はログをモニターするパソコンから算出しています。日時表示がおかしい場合は、パソコンの時計日時を確認、修正し、ログを再表示させてください。

- 再起動するとログ情報は消去されます。
- 各表示画面最下部の［ログ保存］をクリックすると、ファイルのダウンロード画面が表示されます。保存する場所とファイル名を指定して表示内容を保存できます。

■ IPv4／IPv6フィルタリングログ

フィルタリング設定の画面で「ログ出力」にチェックをつけたエントリーがパケットの処理を行うとパケットの情報を記録します。パケット情報は、対象接続、フィルター番号、ステータス、方向、送信元／あて先ポート番号などで、最新の情報(4000件まで)を見ることができます。IPv6接続を行っているときは、IPv6フィルタリングログを見ることができます。

1 設定画面上の［ログ表示］をクリックする

2 フィルタリングログの［表示］をクリックする

3 ［再読み込み］をクリックし、最新のログ画面を表示させる

記録したログを削除するには、［ログ削除］をクリックしてください。

- 再起動するとログ情報は消去されます。
- 各表示画面の一番下にある［ログ保存］をクリックすると、ファイルのダウンロード画面が表示されます。保存する場所とファイル名を指定して表示内容を保存できます。

フィルタリングログのフィルター番号に、"G-P"、"P-P"、"SHR"、"W-C"、"W-P"、"STL"、"STL (Indent)"、"SPI"、"DoS"、"GOR"と表示されている場合、セキュリティワンタッチ設定によるフィルタリングの内容を表示しています。詳しくは96、97、102ページを参照してください。

■ UPnP™ログ(一般)およびUPnP™ログ(CP機能)

UPnP™ログ(一般)は、ポートマッピングの追加、削除、失敗状況のログ情報を一覧で表示します。UPnP™ログ(CP機能)は、UPnP™ CP機能のポートマッピングの追加、削除、失敗のログ情報を一覧で表示します。最大保存ログ件数および1画面に表示できるログ件数は400件です。

1 設定画面上の [ログ表示] をクリックする

2 UPnP™ログの [表示] をクリックする

3 [再読み込み] をクリックし、最新のログ画面を表示させる

記録したログを削除するには、[ログ削除] をクリックしてください。

■ 表示項目

項目	説明
No	ログ番号です。最新のものから順に番号が割り振られます。
日時	本製品がポートの操作を行った時間が表示されます。この時間は表示しているパソコンの現在時刻を基に算出しています。表示されている日時がおかしい場合は、パソコンの時刻設定を確認、調整して、上記手順を繰り返してください。
イベント	本製品が行ったポート操作の内容が表示されます。表示される内容は以下のいずれかの項目です。 ・「ポート追加」:ポート情報が追加されました。 ・「ポート追加失敗」:ポートの追加に失敗しました。 ・「ポート削除」 :ポート情報が削除されました。 ・「ポート削除 (ユーザー操作)」:登録されていた情報がユーザーによって削除されました。 ・「ポート削除失敗」 :ポートの削除に失敗しました。 ・ 「ポート一括削除 (ユーザー操作)」 :登録されていた情報がユーザーによって削除されました。 ・「ポート自動削除 (ユーザー設定)」 :UPnP™ポート自動削除設定タイマーで設定された時間が経過しました。 ・「ポート自動削除 (アプリケーション設定)」 :使用中のアプリケーションにより指定された時間が経過しました。 ・「ポート追加失敗 (無期限指定のみ)」:ポートの追加に失敗しました。 ・「ポート追加失敗 (外部ポート指定制限)」:ポートの追加に失敗しました。
クライアント側 (IPアドレス、ポート)	設定されたポート情報のクライアント側IPアドレスとポート番号が表示されます。
プロトコル	設定された情報の対象となるプロトコルが表示されます。「TCP」もしくは「UDP」が表示されます。
外部ポート	設定されたポート情報の外側(WAN側)のポート番号が表示されます。

情報を知る

■ 接続／切断ログ

PPPoE接続やDHCP接続における接続・切断および認証のログを表示します。接続ログの場合は、接続した際のIPアドレスが確認できます。1画面に100件のログを表示でき、最大400件のログを記録できます。100件以上のログがある場合は、画面下部に記録されているページ番号を選び、目的の情報を表示してください。

1 設定画面上の ログ表示 をクリックする

2 接続／切断ログの 表示 をクリックする

■ みえますねっとログ

みえますねっとサーバーとの通信のログを表示します。1画面に100件のログを表示でき、最大400件のログを記録できます。ログは100件ごとに4グループに分割されています。

1 設定画面上の ログ表示 をクリックする

2 みえますねっとログの 表示 をクリックする

■ VPN（PPTP）接続／切断ログ

VPN 接続／切断ログを400件登録できます。1画面に100件のログを表示でき、最大100件のログを記録できます。

1 設定画面上の ログ表示 をクリックする

2 VPN 接続／切断ログの 表示 をクリックする

■ メール送信ログ

IPアドレス通知によるメール転送のログを表示します。1画面に100件のログを表示でき、最大100件のログを記録できます。ログは100件まで表示できます。

1 設定画面上の ログ表示 をクリックする

2 メールログの 表示 をクリックする

■ IPv6 IPsecログ

IPv6 IPsecの接続情報を確認できます。IPv6接続を行っているときだけ表示されます。1画面に100件のログを表示でき、最大400件のログを記録できます。100件以上のログがある場合は、画面下部に記録されているページ番号を選び、目的の情報を表示してください。

1. 設定画面上の ログ表示 をクリックする
2. IPv6 IPsecの 表示 をクリックする

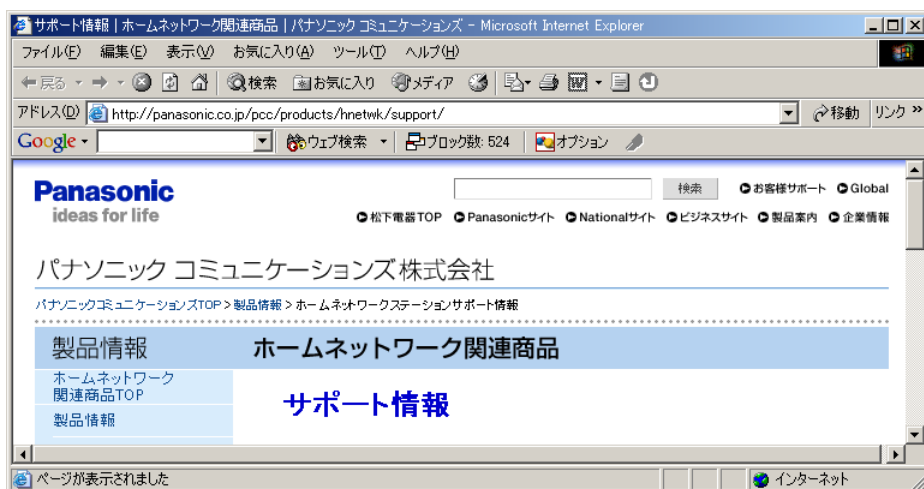
サポートを使う

製品やサポートに関する情報を、インターネットから得ることができます。

1 メニュー画面上の サポート をクリックする

2 製品情報、または、サポート情報のURLをクリックする

ウェブサイトが表示されます。

サポート情報のウェブサイト例

ヘルプを使う

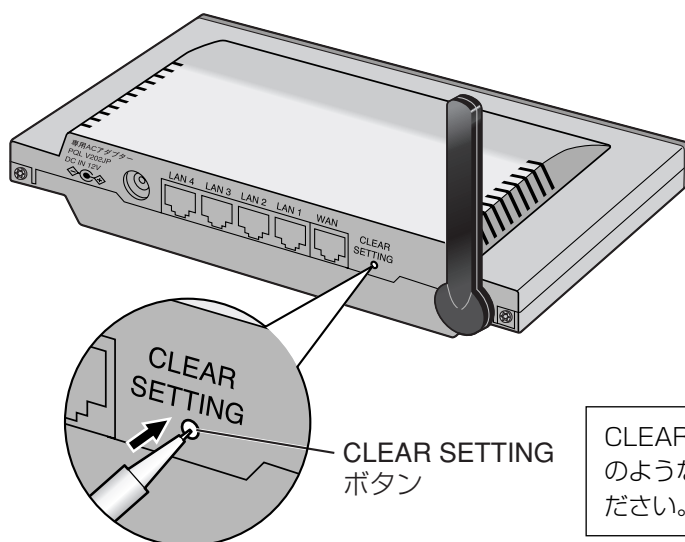
ヘルプ機能は、設定画面の各項目を説明しています。

1 設定画面上の ヘルプ をクリックする

2 調べたい項目を選ぶ

設定画面上の項目をクリックすることでもヘルプを参照できます。

初期化

本製品の背面にCLEAR SETTINGボタンがあります。このボタンは初期化するときに押します。

初期化

パスワード(☞ かんたんガイド)を忘れたり、設定値を工場出荷時の状態(工場出荷時設定 ☞ 165ページ)に戻すときは、CLEAR SETTINGボタンを1秒間押し続けてください。

- CLEAR SETTINGボタンを押すと、設定した内容は消去され工場出荷時設定になります。
- DHCPサーバー機能(☞ 108ページ)を使うときは、本製品に接続しているLAN(ホーム)側のすべてのパソコンを再起動してください。

CLEAR SETTINGボタンでの初期化とメニュー画面での初期化とは、同じ機能です。

再起動

POWERインジケーターが赤に点滅した場合(☞ 「ご使用の前に／困ったときには」の14ページ)は、本製品を再起動してください。コンセントからACプラグを抜き、もう一度差し込むと本製品の設定内容を変更することなく再起動することができます。

DHCPサーバー機能(☞ 108ページ)を使うときは、本製品に接続しているLAN(ホーム)側のすべてのパソコンを再起動してください。

パソコンのUPnP™設定

本製品はUPnP™に対応したアプリケーションやUPnP™対応機器を利用できます。UPnP™機能は、有線で接続したパソコン、無線で接続したパソコンのいずれからでも利用できます。

■ UPnP™について

UPnP™ Forum IGD（Internet Gateway Device）1.0に準拠し、NATトラバーサル機能※に対応しています。これによって、本製品のLAN側に接続した複数台のパソコンから同時にWindows／MSN Messengerを利用できます。

※NATトラバーサル機能
ネットワーク認識アプリケーションが、NATデバイスの配下にあることを検出し、外部IPアドレスを識別して、外部ポートから内部ポートへパケットを転送するポートマッピングを設定できる一連の機能のことです。

■ UPnP™機能を利用できるOS

UPnP™機能に対応しているOSは以下のとおりです。

- Windows XP
- Windows Me

Windows 2000とWindows 98SEは、MSN Messengerを利用することで本製品のUPnP™機能を利用することができますが、UPnP™の正式対応OSではないため、動作を保証するものではありません。

■ UPnP™対応アプリケーション

動作を確認しているUPnP™対応アプリケーションは以下のとおりです。

- MSN Messenger 6.1以降、Windows Messenger 4.7以降（Windows XP）
  Windows MessengerはWindows XPに標準搭載されており、MSN Messengerはマイクロソフトのウェブサイトからダウンロードできます。「インスタントメッセージ」、「音声チャット」、「ビデオチャット」、「ファイルまたは写真の送信」、「リモートアシスタンス」、「アプリケーション共有」、「ホワイトボード」、「電話をかける」(MSN Messengerのみ) などの機能があります。
- MSN Messenger 6.1以降（Windows XP以外）
  Windows 2000またはWindows 98SE／Meで利用可能です。「インスタントメッセージ」、「音声チャット」、「ファイルまたは写真の送信」、「電話をかける」などの機能があります。

- Windows／MSN Messengerを利用するパソコンには、DirectX® 8.1以降がインストールされている必要があります。
- 「電話をかける」機能を利用する場合には、マイクロソフトのウェブサイトから“Windows Messengerのオーディオに関連するアップデート”を行う必要があります。

パソコンのUPnPTM設定

■ UPnPTM機能を利用できるパソコンの台数

UPnPTM機能を利用できるパソコンの台数は、ご使用になるアプリケーションによって左右されます。

UPnPTMで設定可能なポートマッピング数は全セッションの合計で最大128件です。

■ パソコンの準備

＜Windows XPの場合＞

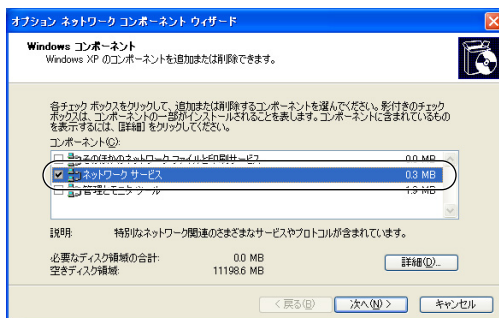
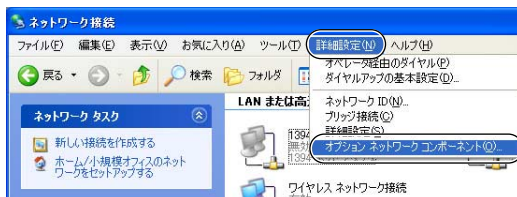
● **Windows Messengerを利用する場合**
Windows Messengerのヘルプメニューから「Windows Messengerのバージョン情報」を選びます。

● **MSN Messengerを利用する場合**
MSN Messenger (Windows XP版) をマイクロソフトのウェブサイトからダウンロードしてインストールしてください。
MSN Messengerのバージョンが6.1より古い場合にはバージョンアップしてください。

UPnPTMの設定

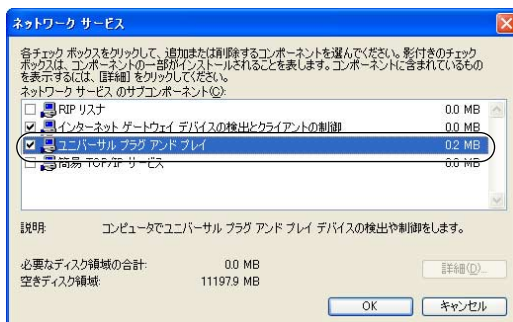
1 「スタート」メニューの「マイコンピュータ」から「マイネットワーク」を選び、「ネットワーク接続を表示する」を選ぶ

2 「詳細設定」メニューから「オプションネットワークコンポーネント」を選ぶ

3 「ネットワークサービス」を選び 詳細 をクリックする

4 「ネットワークサービス」の画面で「ユニバーサルプラグアンドプレイ」にチェックが入っているか確認する

チェックが入っていない場合は、チェックを入れて OK をクリックします。
Windows XPのCD-ROMを要求されたときは、画面の指示に従って操作してください。

パソコンのUPnP™設定

＜Windows 2000、Windows Me、Windows 98SEの場合＞

MSN Messengerのバージョンを確認する

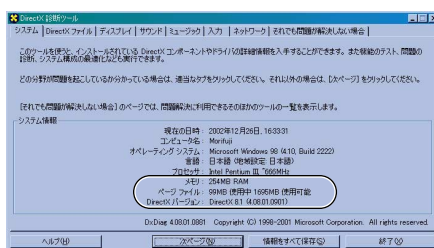
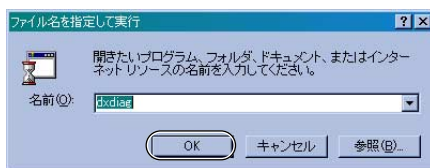
MSN Messengerのヘルプメニューから「MSN Messengerのバージョン情報」を選びます。MSN Messengerのバージョンが6.1より古い場合にはバージョンアップしてください。

DirectXのバージョン確認

1 「スタート」メニューの「ファイル名を指定して実行」を選ぶ

2 名前欄に「dxdiag」を入力して OK をクリックする

3 DirectXのバージョンが8.1より古い場合はバージョンアップする

画面に従って操作してください。

UPnP™の設定（Windows Meのみ設定）

Windows 2000、Windows 98SEにはこの設定はありません。

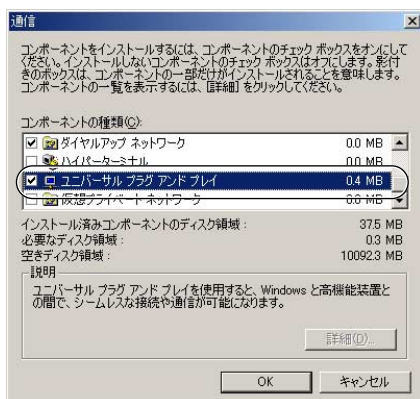
1 「スタート」メニューの「設定」から「コントロールパネル」を選ぶ

2 「アプリケーションの追加と削除」をダブルクリックして、「Windowsファイル」タブをクリックする

3 「コンポーネントの種類」で「通信」を選び 詳細 をクリックする

「コンポーネントの種類」の画面で「ユニバーサルプラグアンドプレイ」にチェックが入っているか確認してください。
チェックが入っていない場合は、チェックを入れて OK をクリックします。
Windows MeのCD-ROMを要求されたときは、画面の指示に従って操作してください。

パソコンのUPnPTM設定

■ その他

<動作環境>

UPnPTMでWindows／MSN Messengerを利用する場合、通信する相手の環境によって動作環境に制約があります。

Windows／MSN Messenger機能を使う際、通信相手がUPnPTMに対応していないルーターを使用している場合や、プライベートアドレスを付与するプロバイダー経由で接続している場合などのように、環境によっては通信できない場合があります。

<本製品接続時のパソコン画面について>

次の手順はWindows XPを使った場合です。

1 本製品にUPnPTMがONに設定されたパソコンを接続する

パソコンのマイ ネットワーク上とタスクトレイ上に本製品のアイコンが表示されます。

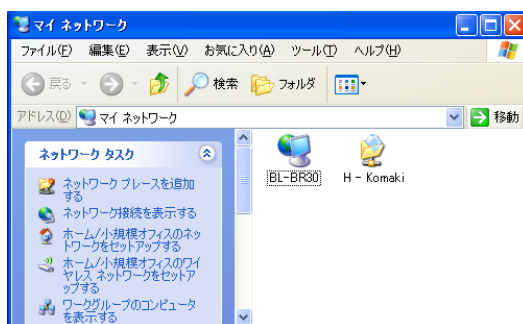
- アイコンは、Windows 2000、Windows 98SEでは表示されません。
- タスクトレイアイコンは一度だけ表示され、二度目の接続では表示されません。

2 マイ ネットワーク上のアイコンをクリックする

- 必要に応じてデスクトップにショートカットを作成してください。

3 マイ ネットワーク上のアイコンをダブルクリックする

ネットワークパスワードの入力画面が表示されます。ユーザー名とパスワードを入力すると、本製品の設定画面が表示されます。

つづく

パソコンのUPnP™設定

機能名称	Windows XP		Windows Meの場合
	Windows Messenger 4.7	MSN Messenger 6.1	MSN Messenger 6.1
インスタントメッセージ	設定によらず使用可	設定によらず使用可	設定によらず使用可
音声チャット	使用可	使用可	使用可
ビデオチャット	使用可	使用可	機能なし
ファイルまたは写真の送信	使用不可※1	使用可	使用不可※1
ホワイトボード	使用可	使用可	機能なし
アプリケーション共有	使用可	使用可	機能なし
リモートアシスタンス	使用可	使用可	機能なし
電話をかける	機能なし	使用可※2	使用可※2

※1 接続環境によっては、受信のみできる場合があります。
※2 本製品を経由した過去の通信や、サーバーの状態により電話ができないと判断される場合があります。

Windows／MSN Messengerの各機能については、Windows／MSN Messengerのヘルプを参照してください。

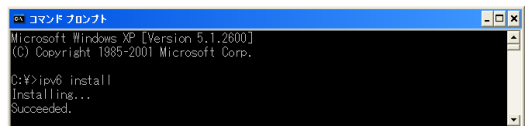
パソコンのIPv6設定

Windouws XPにアドレスを設定する

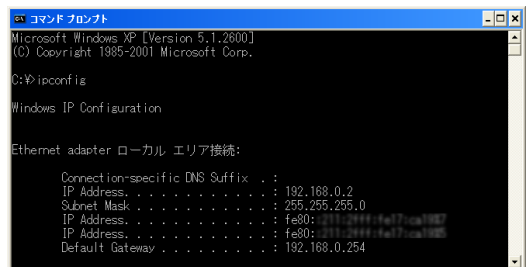
1 [スタート]→[すべてのプログラム]→[アクセサリ]→[コマンド プロンプト]を選びクリックする

● コマンド プロンプトが起動します。

2 "ipv 6 install"と入力し、 Enter を押す

● "Succeeded"と表示されたら、成功です。

Windows XP Service Pack 1がインストールされていないときは、"Succeeded"と表示されません。Service Pack 1をインストールしてください。

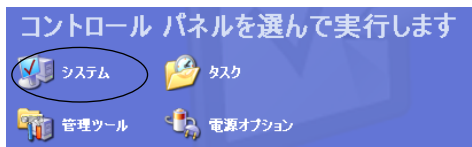
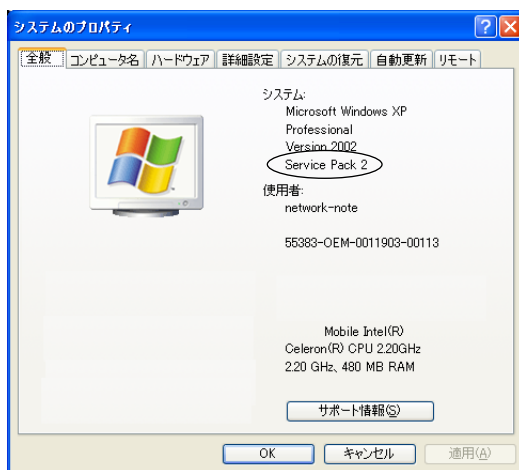
3 コマンド プロンプト画面に"ipconfig"と入力し、 Enter を押す

● IPv6アドレスが表示されたら、パソコンにIPv6アドレスが割り振られているということです。

Windows XP Service Pack 2を使用している場合、IPv6アドレスが設定できないことがあります。以下のステップで使っているパソコンがWindows XP Service Pack 2であるかを確認してください。

1 [スタート]→[コントロールパネル]を選びクリックする

2 パフォーマンスとメンテナンスのアイコンをダブルクリックする

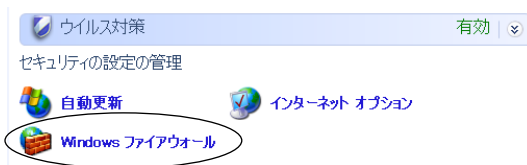
つづく

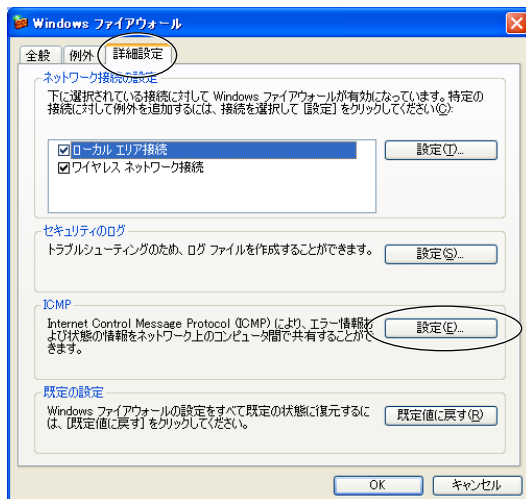
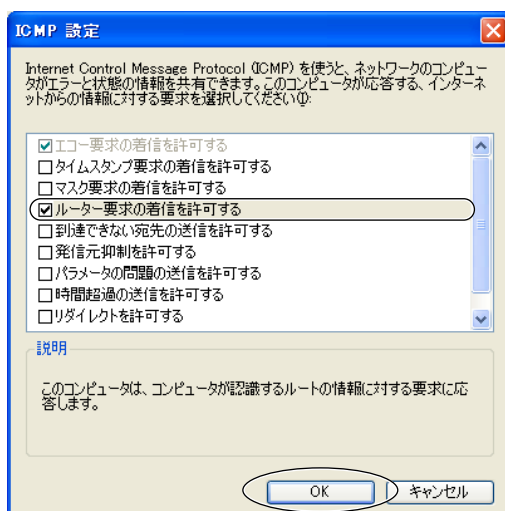
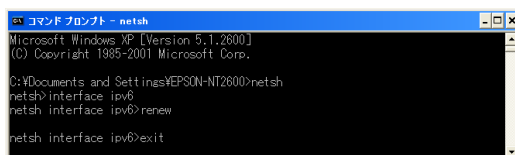
3 システムのアイコンをダブルクリックする

4 「全般」をクリックし、システムが「Service Pack 2」になっているか確認する

Windows XP Service Pack 2を使用している場合は、以下のステップの設定を行ってください。

1 [スタート]→[コントロールパネル]を選びクリックする

2 セキュリティ センターのアイコンをクリックする

3 Windows ファイアウォールのアイコンをクリックする

つづく

パソコンのIPv6設定

4 「詳細設定」タブをクリックし、ICMPの 設定 をクリックする

5 ICMP設定画面で「ルーター要求の着信を許可する」にチェックを入れ、 OK をクリックする

パソコンのIPv6設定

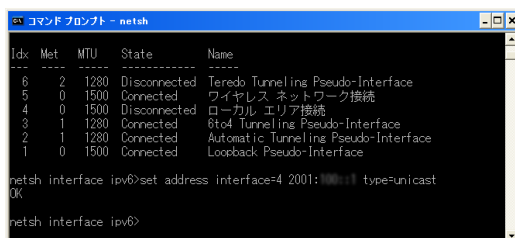
IPv6グローバルアドレスを再取得する

1 [スタート]→[すべてのプログラム]→[アクセサリ]→[コマンド プロンプト]を選びクリックする
- コマンド プロンプトが起動します。

2 "netsh"と入力し、 Enter を押す

3 netshのコマンドラインで、"interface ipv6"、と入力し、 Enter を押す

4 "renew"と入力し、IPv6グローバルアドレスを再取得する

5 "exit"と入力し、 Enter を押し、netshコマンドを終了する

IPv6グローバルアドレスを固定で設定する

1 上記「IPv6グローバルアドレスを再取得する」の手順1、2、3を行う

2 "show interface"と入力し、 Enter を押す
- ローカルエリア接続表示された行の"Idx"の数字を控えておきます。

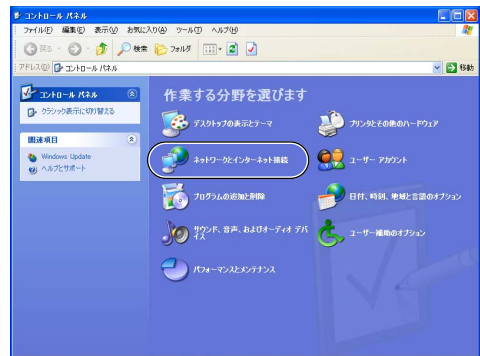
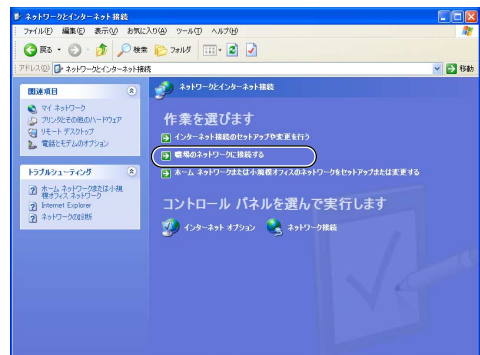
3 続いて"set address interface=* 設定するIPv6グローバルアドレス type=unicast"と入力し、 Enter を押す
- "interface="のあとに設定する番号は、手順3で調べた"Idx"の数字を設定します。

4 "exit"と入力し、 Enter を押し、netshコマンドを終了する

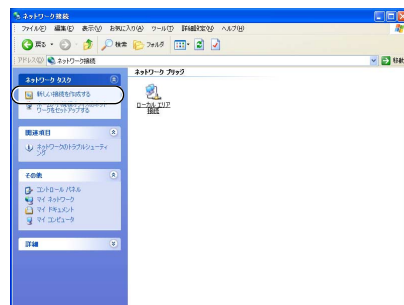
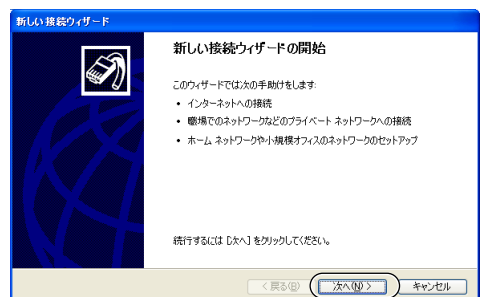
```
コマンド プロンプト - netsh

Idx  Met   MTU    State          Name
---  ----  -----  ------------   -----
  6     2   1280  Disconnected   Teredo Tunneling Pseudo-Interface
  5     0   1500  Connected      ワイヤレス ネットワーク接続
  4     0   1500  Disconnected   ローカル エリア接続
  3     1   1280  Connected      6to4 Tunneling Pseudo-Interface
  2     1   1280  Connected      Automatic Tunneling Pseudo-Interface
  1     0   1500  Connected      Loopback Pseudo-Interface

netsh interface ipv6>set address interface=4 2001:[illegible] type=unicast
OK

netsh interface ipv6>
```

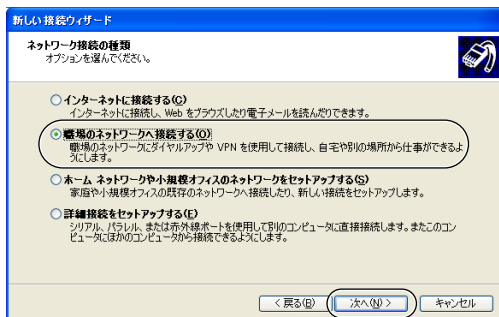
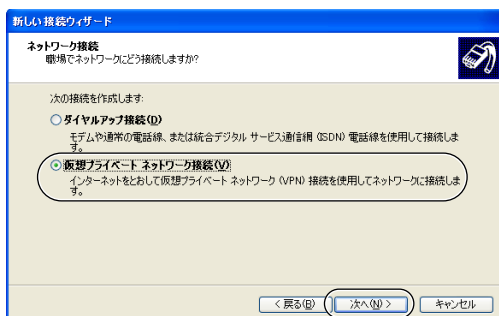
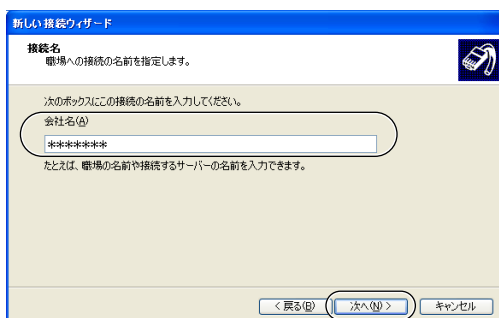
VPN使用時のPPTP設定: Windows XPの場合

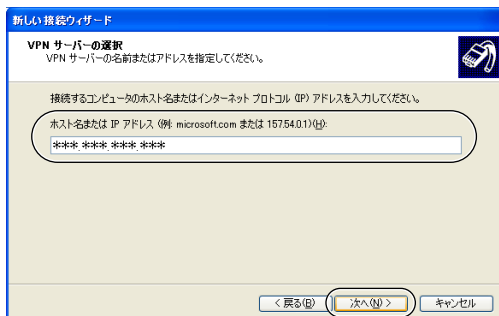
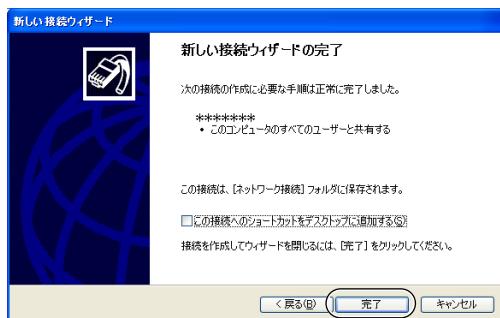
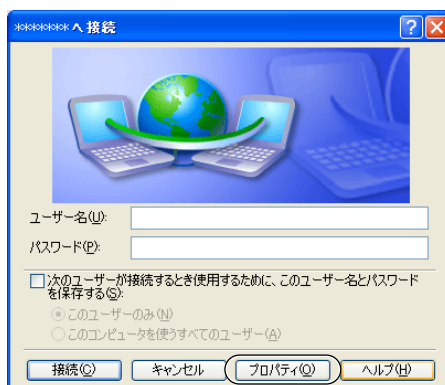
パソコンにVPN(PPTP)接続の設定を行います。Windows XPをご使用の場合、次の手順に従って設定を行ってください。

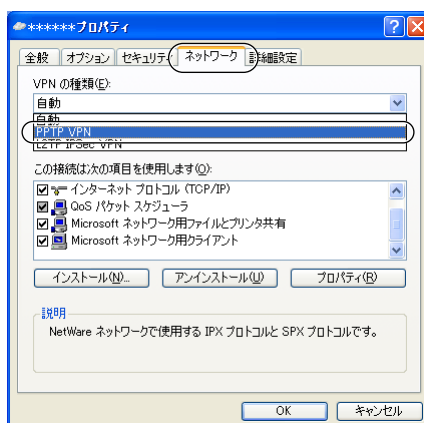
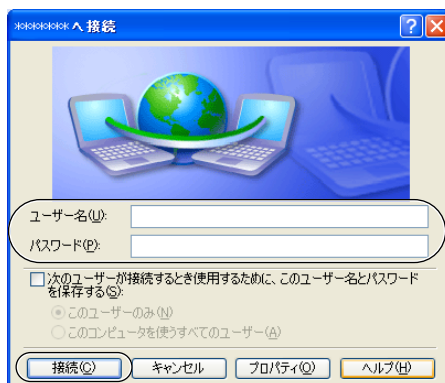
1 スタート メニューの**「コントロールパネル」**から、**「ネットワークとインターネット接続」**をクリックする

2 **「ネットワーク接続」**をクリックする

3 **「新しい接続を作成する」**をクリックする

4 次へ をクリックする

つづく

VPN使用時のPPTP設定: Windows XPの場合

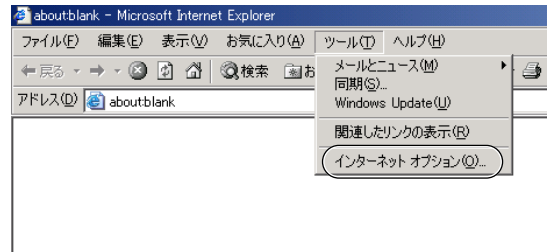
5 「職場のネットワークに接続する」をチェックし、 次へ をクリックする

6 「仮想プライベート ネットワーク接続」をチェックし、 次へ をクリックする

7 任意の接続名を入力し、 次へ をクリックする

8 本製品WAN側IPアドレスを入し、 次へ をクリックする

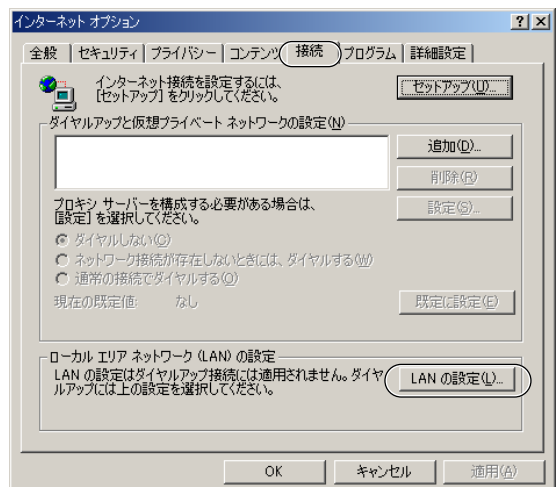
つづく

9 完了 をクリックする

10 プロパティ をクリックする

11 **ネットワーク**タブをクリックし、「VPNの種類」のドロップダウンリストから**「PPTP VPN」**を選び、 OK をクリックする

セキュリティでの設定と**オプション**での設定を、本製品に設定した認証方式と暗号化方式(☞ 121ページ)に合わせて設定してください。

12 本製品に登録した**ユーザー名**と**パスワード**を入力し、 接続 をクリックする

プロキシサーバー使用時のウェブブラウザの設定

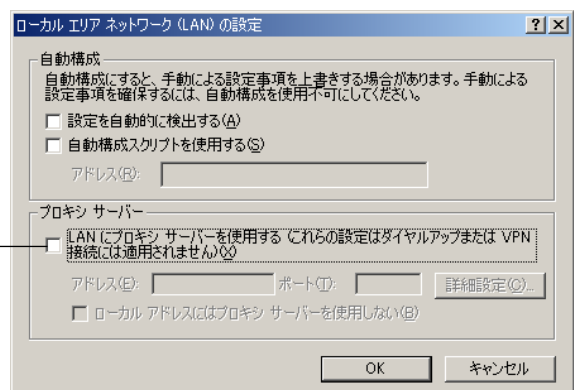
プロバイダーによっては、プロキシサーバーを経由してインターネットに接続する場合があります。
プロキシサーバーを経由する場合は、設定画面にアクセスすることはできません。次の手順に従ってウェブブラウザの設定を変更してください。

次の手順は、Internet Explorer 6.0を使った場合です。

1 ウェブブラウザを起動する

2 **「ツール」**メニューから**「インターネット オプション」**を選ぶ

3 **接続**タブをクリックする

4 LAN の設定 をクリックする

5 **ローカル エリア ネットワーク(LAN)の設定**ダイアログボックスで、**「LAN プロキシ サーバーを使用する」**のチェックボックスを確認する

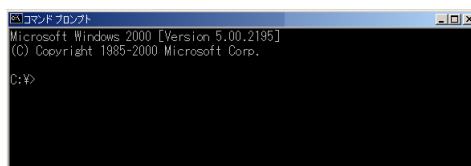
- **チェックボックスがチェックされていたら、**チェックをはずして OK をクリックしてください。
- **チェックボックスがチェックされていなかったら、** キャンセル をクリックし設定を終了してください。

チェックボックスがチェックされていないことを確認してください。

パソコンのIPアドレスやMACアドレスを確認するには

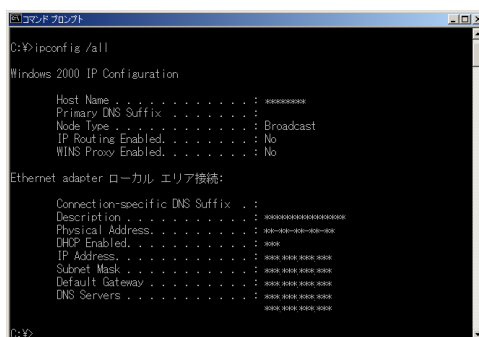
各パソコンから本製品の設定画面にアクセスできない、またはネットワーク上の他のパソコンと通信できない、などの場合には、各パソコンのIPアドレスの設定に問題がある可能性があります。以下の手順に従ってIPアドレスの設定を確認してください。

Windows XP／2000の場合

1 スタート メニューから**「すべてのプログラム」、「アクセサリ」、「コマンド プロンプト」**を選ぶ

Windows 2000の場合は、スタート メニューから**「プログラム」、「アクセサリ」、「コマンド プロンプト」**を選んでください。

2 **コマンドプロンプト**のあとに**ipconfig /all**と入力し、Enterキーを押す

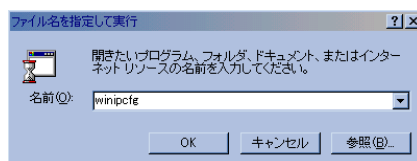
● **ipconfig/renew_all**について
すべてのLANカードのDHCP構成パラメーターを更新します。

● **ipconfig/release_all**について
すべてのLANカードのDHCP構成パラメーターを解放します。

ipconfigコマンドの説明は、コマンドプロンプトのあとにipconfig/？と入力すると表示されます。

Windows Me／98SEの場合

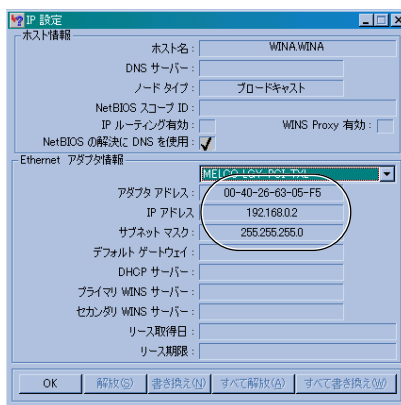
以下の手順は、Windows 98SEの場合です。

1 スタート メニューから**「ファイル名を指定して実行」**を選ぶ

つづく

2 **名前**欄に**winipcfg**と入力し、[OK]をクリックする

3 IPアドレスを確認したいLANカード(イーサネットアダプタ)を選ぶ

4 [詳細]をクリックする

IPアドレス欄を見て、設定されているIPアドレスを確認してください。
アダプタ アドレス欄を見て、LANカード(イーサネットアダプタ)のMACアドレスを確認してください。

「IPアドレスを自動的に取得」を設定していて、「169.254.XXX.X」などの値が表示された場合は、IPアドレスが正しく取得できていない可能性があります。そのような場合は、次の手順に従ってIPアドレスを更新してください。

1 [解放]をクリックする

自動取得していたIPアドレスが解放されます。

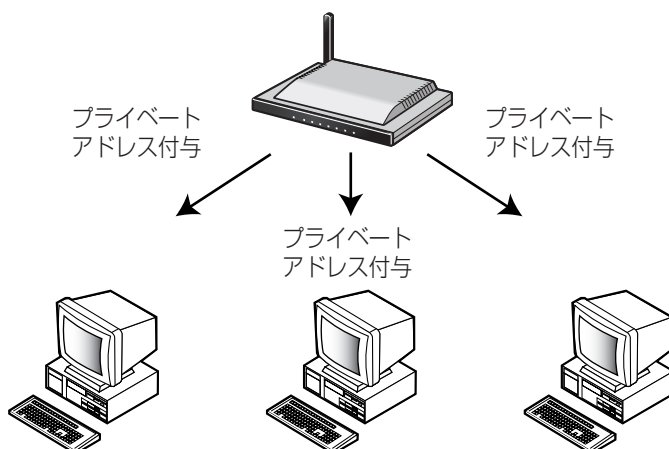
2 [書き換え]をクリックする

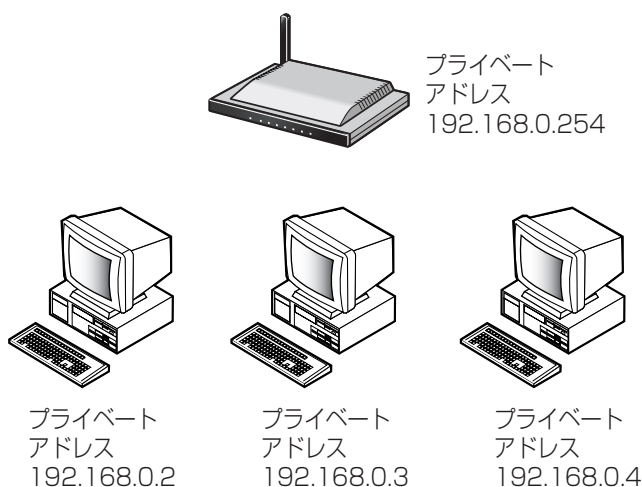
新しいIPアドレスが割り振られます。

3 [OK]をクリックする

パソコンのIPアドレスを固定するには

本製品を含めたTCP/IPネットワークのすべてのパソコンには、それぞれ固有のIPアドレスの設定が必要です。
本製品では、DHCPサーバー機能を使って、LAN（ホーム）側の各パソコンにIPアドレスを自動で割り振ることができます（工場出荷時設定）。この場合、本製品が各パソコンにIPアドレスを割り振ったり、再割り振りするため、各パソコンのIPアドレスは固定していません。

本製品がIPアドレスを割り振るネットワーク（工場出荷時設定）

これに対し、本製品のDHCPサーバー機能を無効にして、LAN側の各パソコンのプライベートアドレスを固定することができます。この場合、あらかじめ各パソコンに固有のIPアドレスを設定する必要があります。

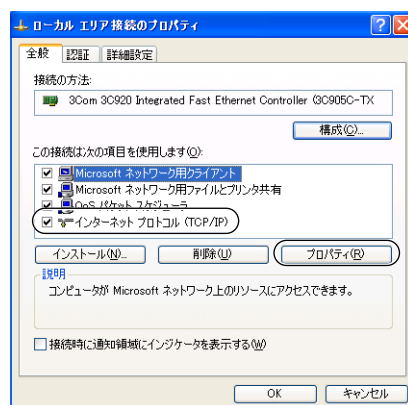
IPアドレスが固定されたネットワーク（オプション設定）
本製品のDHCPサーバー機能を使用せずに、プライベートアドレスを固定してネットワーク設定を行います。各パソコンに固有のプライベートアドレスを固定して設定する必要があります。各パソコンに固有のプライベートアドレスを設定したあとに、本製品を設定します。108ページを参照し、オプション設定画面上のDHCPサーバー機能を無効にしてください。各パソコンの設定は、161、163ページの手順に従ってください。

パソコンのIPアドレスを固定するには

Windows XP／2000の場合

1 スタート メニューの**「マイ コンピュータ」**から**「マイ ネットワーク」**を選び、**「ネットワーク接続を表示する」**を選ぶ

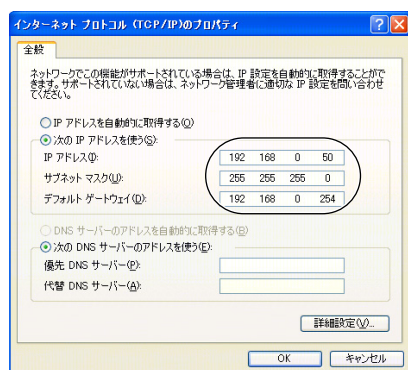
Windows 2000の場合は、**「マイ ネットワーク」**アイコンを右クリックし、**「プロパティ」**を選ぶ

2 本製品が接続されている**「ローカル エリア接続 ...」**アイコンを右クリックし、 プロパティ を選ぶ

3 **「インターネット プロトコル（TCP/IP）」**を選び、 プロパティ をクリックする

4 **「次のIP アドレスを使う」**を選ぶ

5 各パソコンのIPアドレス（例：192.168.0.50）とサブネットマスクを入力し、**192.168.0.254**（本製品の工場出荷時設定IPアドレス）を**「デフォルト ゲートウェイ」**の入力欄に入力する

サブネットマスクは通常255.255.255.0と入力します。本製品の設定画面にアクセスする場合は、本製品のサブネットマスクと同じ値を入力してください。

つづく

パソコンのIPアドレスを固定するには

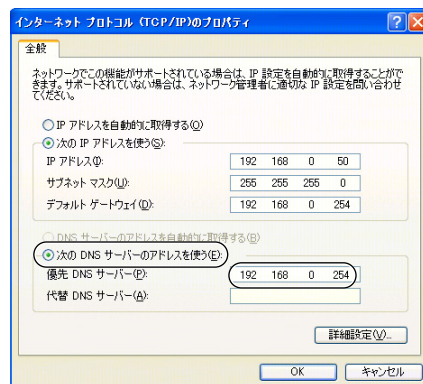
6 **「次の DNS サーバーのアドレスを使う」**をクリックする

7 DNSサーバーのアドレスを入力欄に入力し、[OK] をクリックする

8 [閉じる] をクリックする

Windows 2000の場合は、[OK] をクリックしてください。

9 **「ネットワーク接続」**のウィンドウを閉じて、パソコンを再起動する

Windows 2000の場合は、**「ネットワークとダイヤルアップ接続」**のウィンドウを閉じて、パソコンを再起動してください。

パソコンのIPアドレスを固定するには

Windows Me／98SEの場合

1 スタート メニューから**「設定」**を選び、**「コントロール パネル」**をクリックする

2 **「ネットワーク」**アイコンをダブルクリックする

Windows Meで**「ネットワーク」**アイコンが見つからない場合は、**「すべてのコントロールパネルのオプションを表示する」**をクリックしてください。

3 **ネットワーク**ダイアログボックスで、本製品に接続しているLANカードに関連したTCP/IPを選び、 プロパティ をクリックする

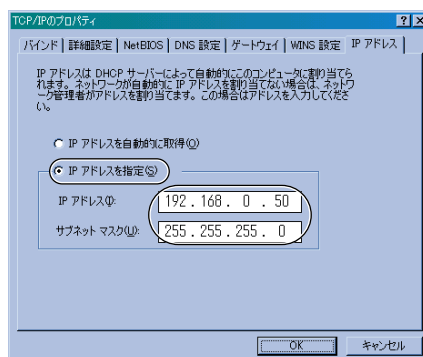
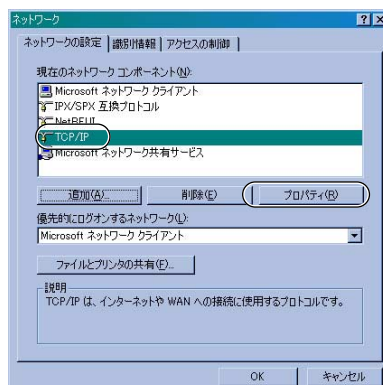
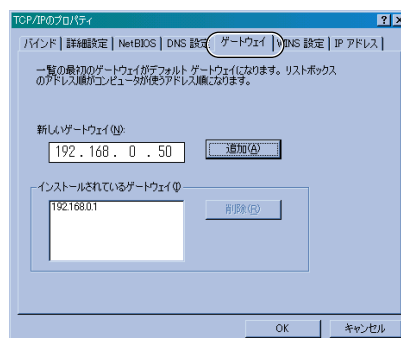
TCP/IPのプロパティダイアログボックスが表示されます。

4 **TCP/IPのプロパティ**ダイアログボックスで、**IP アドレス**タブをクリックする

5 **「IP アドレスを指定」**を選ぶ

6 各パソコンのIPアドレス（例：192.168.0.50）とサブネットマスクを入力する

サブネットマスクは通常255.255.255.0と入力します。本製品の設定画面にアクセスする場合は、本製品のサブネットマスクと同じ値を入力してください。

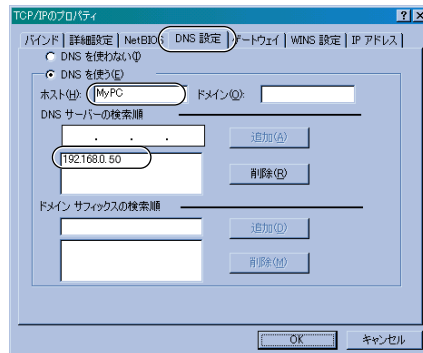
つづく

7 **ゲートウェイ**タブをクリックする

8 192.168.0.254（本製品の工場出荷時設定IPアドレス）を**「新しいゲートウェイ」**のアドレス欄に入力し、**追加** をクリックする

9 192.168.0.254が**「インストールされているゲートウェイ」**のアドレス欄に入力されていることを確認する

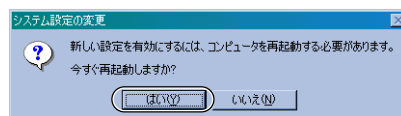
本製品のIPアドレスを変更する場合は、**「インストールされているゲートウェイ」**のIPアドレスも変更してください。

10 **DNS 設定**タブをクリックする

11 **「DNS を使う」**を選ぶ

12 DNSサーバーアドレスを**「DNS サーバーの検索順」**のアドレス欄に入力し、**追加** をクリックする

13 任意のホスト名を入力し、OK をクリックする

14 OK をクリックする

システム設定の変更ダイアログボックスが表示されます。

15 **はい** をクリックし、パソコンを再起動する

工場出荷時設定一覧

プロバイダー登録

プロバイダー登録モニター	No.1 No.2 No.3 No.4	DHCP接続 未登録 未登録 未登録

IPv6プロバイダー登録

プロバイダー登録モニター	No.1 No.2 No.3 No.4	未登録 未登録 未登録 未登録

接続設定管理

WAN(インターネット)側接続モード	DHCP／Static
プロバイダー設定	DHCP

カメラ設定

カメラ登録 カメラの自動登録機能の設定 IPv4 利用可能なアドレス範囲 カメラに設定するポート番号 利用可能なポート範囲	 使用する 192.168.0.151－192.168.0.166 範囲指定 60001－60016
カメラモニター画面配置 カメラモニター画面表示形式	 カメラ名と静止画 (自動更新)

つづく

工場出荷時設定一覧

無線設定

基本 　通信モード 　SSID 　無線ステルス機能 　通信チャンネルの設定	 802.11b/g (本製品背面に記載) 使用する (ANYキーによる接続も拒否されます) 7
暗号化 　暗号化方式 　WEPキー1	 WEP方式 (本製品背面に記載)
MACアドレスフィルタリング	使用しない

みえますねっと設定

みえますねっと設定	使用しない

アドレス変換

有効／無効の設定 DHCP／Static接続 PPPoE接続 　メインセッション 　サブセッション 端末型 　DMZ機能 (端末型) LAN型 　DMZ機能 (LAN型)	 使用する 使用する 使用する 設定されていません 設定されていません

つづく

工場出荷時設定一覧

セキュリティ設定

セキュリティ 　セキュリティワンタッチ設定	● G-IPからP-IPへの通信を禁止する。(ログ出力) ● プライベートアドレスでのアクセスを双方向に禁止する。(ログ出力) ● NetBIOS／ファイル共有／プリンター共有／PCリモートのアクセスは双方向に禁止する。(ログ出力)
アクセス制限 　設定画面 　カメラモニター画面 　ステルスモードの設定 　不正アクセス検知	● 禁止する。(ログ出力) ● パスワードなしで許可する。(ログ出力) ● 本製品の存在をWAN (インターネット) 側から検知できないようにする。(Identパケットは例外とする。) (ログ出力) ● ステートフル・パケット・インスペクション(動的パケットフィルタリング)を使用する。(ログ出力)
フィルタリング 　フィルタリング設定条件	設定されていません

IPv6セキュリティ設定

セキュリティ 　IPv6セキュリティワンタッチ設定 　ステルスモードの設定 　IPv6不正アクセス検知	● ダイレクトホスティングSMBのアクセスだけは双方向に禁止する。(ログ出力) ● RPCに利用されるポートのアクセスだけは双方向に禁止する。(ログ出力) ● 割り当てグローバルアドレス以外のアドレスを使った通信を禁止する。(ログ出力) ● 本製品の存在をWAN（インターネット）側IPv6ネットワークから検知できないようにする。（Identパケットは例外とする。）（ログ出力） ● ステートフル・パケット・インスペクション(動的パケットフィルタリング)を使用する。(ログ出力)
IPv6フィルタリング 　IPv6フィルタリング設定条件	設定されていません

つづく

工場出荷時設定一覧

オプション設定

<table>
<tr><td>LAN(ホーム)側IPアドレス設定
IPアドレス
サブネットマスク
設定画面のポート番号
カメラモニター画面のポート番号

DHCPの設定
DHCPサーバー
利用可能なアドレス範囲

DHCPスタティック設定</td><td>
192.168.0.254
255.255.255.0
8080
80

使用する
192.168.0.1－192.168.0.32

無効</td></tr>
<tr><td>PPPoE設定
メインセッション
サブセッション</td><td>
常時接続
常時接続</td></tr>
<tr><td>DNSリレー設定</td><td>使用する</td></tr>
<tr><td>MTU設定</td><td>1500バイト (DHCP／Static接続)
1492バイト (PPPoE接続)</td></tr>
<tr><td>ダイナミックルーティング設定
LAN(ホーム)側設定
WAN(インターネット)側設定

スタティックルーティング設定</td><td>
使用しない
使用しない

設定されていません</td></tr>
<tr><td>UPnP機能
IGD機能
CP機能

UPnPポート自動削除設定
タイマー</td><td>
使用する
使用する

無期限</td></tr>
<tr><td>IPアドレス通知
メール設定(共通)
メールあて先設定</td><td>使用しない
設定されていません
設定されていません</td></tr>
</table>

つづく

工場出荷時設定一覧

IPv6オプション設定

LAN（ホーム）側IPv6アドレス設定 RA（LAN側IPv6自動設定）の設定	fe80::254 送信する
リンクMTUサイズ	1500バイト
IPv6ダイナミックルーティング設定 　WAN側 　LAN側 IPv6スタティックルーティング設定	 使用しない 使用しない 設定されていません

VPN(PPTP)設定

基本 　PPTPサーバー 　利用可能なアドレス範囲 ユーザー登録 詳細 　認証方式の設定 　暗号化方式の設定	 使用しない 192.168.0.100-192.168.0.101 設定されていません 使用しない MS-CHAP、またはMS-CHAPv2を使用する MPPE40 bitまたは、MPPE128 bitを許可する

VPN（IPsec）設定

IPsecの設定 セキュリティポリシー・データベース登録	使用しない 設定されていません

パスワード設定

設定画面	本製品に初めてアクセスするときに設定します
カメラモニター画面	設定されていません

用語解説

英字

CATV	Cable Televisionの略で、ケーブルテレビのことです。 最近では、このケーブルテレビの回線を使ってインターネットに接続するサービスを提供する会社が増えてきています。
DHCP (Dynamic Host Configuration Protocol)	各パソコンがネットワークを利用するのに必要な情報をサーバーから自動的に取得するプロトコルです。DHCPサーバーは、IPネットワークに関連した情報(IPアドレスの割り振り範囲やデフォルトゲートウェイなど)を保持しており、DHCPクライアントから要求がくると、それらの情報を割り振ります。
DMZ	DMZ(De-Militarized Zone)とは、インターネットに接続されたネットワークにおいて、ファイアウォールによって外部のインターネットからも内部のネットワーク(組織内のネットワーク)からも隔離された区域のことを指します。
DNS (Domain Name System)	ネットワーク環境で実際使用されるIPアドレスは、憶えにくく実用的ではありません。その解決法としてパソコンにわかりやすい名前(ドメイン名)をつけて、IPアドレスに変換して通信が行われます。 ドメイン名では、たとえば“panasonic.jp”などがあります。
FTP (File Transfer Protocol)	インターネットやイントラネットなどのTCP/IPネットワークでファイルを転送するときに使われるプロトコル。現在のインターネットでHTTPやSMTP／POP3と並んで頻繁に利用されているプロトコルです。
IEEE 802.11a	IEEE(米国電気電子学会)の無線LANの規格です。802.11aは、5 GHz帯を使用する最高54 Mbpsの高速な無線LANの規格です。
IEEE 802.11b	IEEE(米国電気電子学会)の無線LANの規格です。802.11は赤外線も含む無線ネットワーク全般に関する規格であり、その中の802.11bは2.4 GHz帯を使用する最高11Mbpsのネットワーク規格を定めています。この規格の作成には、米国だけでなく日本やヨーロッパからも参加しています。
IEEE 802.11g	IEEE(米国電気電子学会)の無線LANの規格です。802.11gは、IEEE 802.11bと互換性を持ち、同じ2.4 GHz帯を使いながら、最大で54 Mbpsのデータ通信が行えます。本製品では、IEEE 802.11bと互換性のあるモードを802.11b/gと記載し、IEEE 802.11bと互換性のないモードを802.11g専用と記載しています。
IPsec (アイ・ピー・セック)	IP securityの略です。TCP/IPで用いられるセキュリティ技術です。パケットの暗号化や認証に関するプロトコルが制定されており、セキュリティを強化したサービス提供が可能です。

つづく

IPv4 (アイ・ピー・ブイ・フォー)	Internet Protocol version 4の略です。IPv4は、現在のインターネットで利用されている標準のプロトコルで、32ビットのアドレス空間(42億9496万7296台の端末をサポートできる)をもっています。
IPv6 (アイ・ピー・ブイ・シックス)	Internet Protocol version 6の略です。増加するインターネットの使用者に対応するため、現在のIP(IPv4)に代わるものとしてIETF(Internet Engineering Task Force)内のIPNGワーキンググループで準備が進められてきたプロトコルです。IPv6には、IPアドレスの128ビット化(IPv4は32ビット)、パケットヘッダの簡素化、セキュリティ機能の追加などが盛り込まれています。
IPアドレス (Internet Protocol Address)	IPプロトコルで使用するためのアドレス情報です。IPで通信するすべてのネットワーク機器にはこのIPアドレスを割り振っておかなければなりません。特に、インターネットに接続されているネットワーク機器(端末)では、世界中でユニークな(単一な)IPアドレスを割り振っておく必要があります。
IPマスカレード	IPアドレスを変換する際に、ポート番号も変換する仕組み(NAPT [Network Address and Port Translation])で、インターネットに接続しているネットワークで、1つのグローバルアドレスを複数のプライベートアドレスから利用する技術です。
LAN (Local Area Network)	フロアの中や同一建物内、キャンパスの中など、比較的狭い地域でのコンピューターネットワークのことです。
MACアドレス (Media Access Control Address)	LANカードなどに固有でつけられている物理アドレスのことです。00:11:22:AA:BB:CCといった形式で表されます。同じMACアドレスをもつLANカードは存在しません。すべて異なる物理アドレスが割り振られています。
MPPE (Microsoft Point-to-Point Encryption)	PPPによるダイヤルアップ接続、または、PPTPによるVPN接続のデータを暗号化します。MPPE128 bit(強力)およびMPPE40 bit(標準)の2つの暗号化方式があり、PPTP接続とNAS(ネットワーク・アクセス・サーバー)の間のデータセキュリティを強化します。
MS-CHAP/MS-CHAPv2	MS-CHAPは「Microsoft Challenge Handshake Authentication Protocol」、MS-CHAPv2は「Microsoft Challenge Handshake Authentication Protocol version 2」の略です。これらは、PPP接続時に、ユーザー名とパスワードを暗号化して相手認証を行う暗号化認証方式です。MS-CHAPは、クライアントからNAS(ネットワーク・アクセス・サーバー)への一方向の暗号化を行う認証方式です。これに対し、MS-CHAPv2は、クライアントとNASの双方がそれぞれの身元を証明する相互認証機能をもつほか、強力な初期データ暗号化キー、および送受信での異なる暗号化キーの使用を採用していますので、MS-CHAPよりもセキュリティが向上しています。

つづく

用語解説

MTU (Maximum Transfer Unit)	MTUは、ネットワークにおいて1回の転送で送信できるデータの最大値を示します。
NAT (Network Address Translation)	社内のみで通用するプライベートアドレスと、インターネットアクセスに利用できる本来のグローバルアドレスを相互に変換し、ローカルなIPアドレスしか割り振られていないノードから、透過的にインターネットへアクセスできるようにする技術です。
ONU (Optical Network Unit)	光ファイバー加入者通信網において、パソコンなどの端末機器をネットワークに接続するための装置です。
Open System	IEEE802.11規格では、Open SystemとShared Keyの、2つの認証サービスをサポートしています。Open System方式では暗号鍵を使わずに接続認証を行います。従って、暗号鍵が異なっても無線リンクが成立することがあり、無線リンクはするが通信はできない場合があります。
POP3 (Post Office Protocol Version 3)	インターネットやLANで、Eメールを受信するためのプロトコル。クライアントが、メールサーバーからEメールを受信する際に用いられ、認証機能をもちます。この認証機能をSMTPでEメール送信する場合に、利用するメールサーバーもあります(POP before SMTP)。
PPP (Point to Point Protocol)	公衆回線などを経由して2台のパソコンを接続するために開発されたプロトコルです。ユーザー名、パスワードでの認証機能や圧縮機能をサポートするだけでなく、複数のプロトコルを同時にサポートできます。
PPPoE	PPP over Ethernetの略です。PPPoEは、複数のプロバイダと接続することができます。
PPPoEマルチセッション機能	フレッツなどの複数のPPPoEセッションを利用する際に、複数のプロバイダーへ同時接続したり、フレッツ・スクウェアなどのインフォメーションサイトとプロバイダーへ同時接続することができます。
PPTP (Point to Point Tunneling Protocol)	インターネット上でVPNを実現するためのプロトコルの1つです。PPTPではPPPをベースに、データの暗号化や認証、リンクの確立などの機能をもたせています。
Shared Key	IEEE802.11規格では、Open SystemとShared Keyの、2つの認証サービスをサポートしています。Shared Key方式では接続認証に暗号鍵を使います。従って、暗号化方式にWEP暗号を選択する必要があります。また、暗号鍵が異なっていると接続認証に失敗するため無線リンクは成立しません。

つづく

用語解説

SMTP (Simple Mail Transfer Protocol)	インターネットやLANでEメールを送信するためのプロトコル。サーバー間でEメールの送受信をしたり、クライアントがサーバーにEメール送信する際に用いられます。
SSID	無線ネットワークグループの識別名です。無線接続をグループ分けするためのものです。「ESSID」とも言います。半角英数字記号1～32文字まで入力できます。(英字は大文字、小文字の区別があります。) 自動設定では本製品のSSIDが転送されます。
TCP/IP	Transmission Control Protocol/Internet Protocolの略です。ネットワークプロトコルの1つです。UNIXワークステーションおよびインターネットにおける標準プロトコルです。
UPnP™ (Universal Plug and Play)	UPnP™は、TCP/IPベースでネットワークデバイスの自動検出や情報交換などを行う技術です。UPnP™に対応するアプリケーションには、MSN Messenger 5.0以降、Windows Messenger 4.7以降などがあります。UPnP™ Forumによって仕様が策定されています。
URL (Uniform Resource Locator)	インターネット上のリソースを指定する方式です。具体例としては、インターネット上のウェブサイトにアクセスする際に使用する「http://panasonic.jp」のことです。
VPN (Virtual Private Network)	インターネットでデータ通信を行うと、通常はデータの暗号化やユーザー認証などは行われていないため、内容が第三者に盗聴されたり改ざんされたりする恐れがあります。そこで、インターネットにデータを送信する前にデータを暗号化して送信すれば、セキュリティを確保することができます。この暗号化をユーザーから透過的に行い、かつユーザー認証によってある特定のユーザーだけしかアクセスできないようにすれば、公衆回線網を使っても、専用線接続と同じようなセキュリティを保つことができます。これをVPN(私設仮想回線)と言います。
WEPキー	無線通信における暗号化技術を意味します。第三者によるデータの傍受を防ぐために、送信パケットを暗号化することでセキュリティを高める技術です。 16進数入力の場合は0～9、A～Fもしくはa～fの入力ができます。 英数字入力の場合はアスキー文字の入力ができます。
WEPキーサイズ	64／128／152 bit の暗号化方式が選択できます。 備考：暗号化は、64 bit、128 bit、152 bitの順でセキュリティ強度が高くなります。 逆に、実質の通信速度は、なし、64 bit、128 bit、152 bitの順で遅くなります。
WEP認証方式	IEEE802.11規格では、Open SystemとShared Keyの、2つの認証サービスをサポートしています。

つづく

用語解説

あ

アクセスポイント
プロバイダーやパソコン通信に電話回線で接続する際に、接続できるサーバーのある場所や電話番号のこと。

暗号化
第三者によるデータの傍受を防ぐために、ネットワークの伝送経路で規則に従ってデータを変換することを意味します。暗号化方式には、共通鍵暗号方式(Shared Key)、公開鍵方式(Open System)などがあります。

イーサネット (Ethernet)
Xerox社などによって開発されたLAN通信方式です。

インストール
ハードウェアやソフトウェアをシステムに新しく組み込むことです。たとえば拡張カードを追加したり、OSなどの新しいソフトウェアをシステムに組み込むときに用いられます。

インターネット
地球規模でマルチメディア通信ができるネットワークです。プロバイダーがインターネットへの接続サービスを行っています。

ウェブサーバー
画像、動画、音声などをハイパーテキスト形式で蓄積し、情報を提供するファイルサーバーです。ハイパーテキスト型情報では、情報内のテキスト文字列(ワード)が別の情報であるテキストやファイル、画像、動画、音声などにリンクしているので、それぞれのワードをマウスでクリックすると、より詳しい情報を抽出することができます。

ウェブブラウザ
ウェブサーバーにアクセスするためのクライアント・プログラムです。Microsoft社のInternet Explorerなどがあります。

か

グローバルアドレス (Global address)
インターネットに接続された機器に1つ1つ割り振られたIPアドレスです。インターネット上の住所に相当するもので、インターネット通信の際には必ず使用されます。グローバルアドレスはIANA(Internet Assigned Numbers Authority)が一元的に管理し、各国のNIC(日本ではJPNIC)プロバイダーなどの各組織に割り振られます。

ゲートウェイ
ゲートウェイは、ルーティング情報を交換しネットワークを管理しているコンピューター(ルーターなど)でネットワークのパケットの道先案内をします。ローカルネットワーク以外への通信は、デフォルトゲートウェイを介して行われます。

つづく

さ

サブネットマスク
IPアドレスは、ネットワークIDとホストIDによって構成されます。
そのネットワークIDとホストIDとを区別するために、サブネットマスクがネットワークIDの長さを判定する役目をします。

ステートフル・パケット・インスペクション
送出パケットの情報から戻りパケットを予測して、パケットの通過や破棄を決定する動的なパケットフィルタリング方式です。

ストレートケーブル
通常は、パソコンとイーサネットハブを接続するためのケーブルの種類です。

静的IPマスカレード (ポートフォワーディング)
ポートフォワーディングとは、特定のポートあての通信を指定したポートへ転送することです。 ポートフォワーディングにより、インターネット側からホームネットワークへのアクセスも可能になり、ホームネットワーク上にウェブサーバー、メールサーバーなどを構築することができます。

静的NAT
ネットワーク内で使用するプライベートアドレスと、インターネット上で使用するグローバルアドレスを1対1で相互変換することです。

た

ダイバーシティ
位置が違うところに2つ以上のアンテナを設置し、受信状態のよいアンテナを選択して受信する方式のことです。

ダウンロード
遠隔地にある装置側からネットワークを使用し、データを自分側に転送し保存する作業です。

チャンネル
無線通信で使用できる周波数帯域を分割すると、別々の通信ができます。分割したそれぞれの周波数がチャンネルです。

デフォルトゲートウェイ
内部ネットワークから外部のパソコンへアクセスするために使用する窓口となるルーターなどの機器を意味します。送信先のIPアドレスに特定のゲートウェイを指定していない場合に、デフォルトゲートウェイにデータが送信されます。

ドメイン
インターネットやイントラネットのネットワークで、サーバーを中心としたネットワークを構成するまとまりを表わします。

つづく

な

ネットワーク

情報交換のためにコンピューターなどの各種装置、機器などがケーブルや公衆回線、無線などを介して接続されていることです。

認証方式

本製品では、無線LAN暗号化設定時の認証方式としてShared Key方式、Open System方式に対応しています。

は

パケット

通信データを一定の大きさに分割し、アドレスをつけて転送するときのデータの単位のことです。

パケットフィルタリング（Packet Filtering)

ファイアウォールの一種で、フィルター機能を用いて、ネットワークパケットを選択的に転送する方式のことです。適切に設定すると、不要なパケットが転送されるのを防ぎます。

ハブ

イーサネットで用いられる集線装置です。8ポートや4ポートなど、複数のポート数をもつ装置があります。

パスワード

ファイルやネットワークを利用する際に鍵の役目をする合言葉(文字や数字)です。ネットワークのセキュリティ上、ユーザー識別のためにあらかじめ言葉を登録します。登録されている言葉と一致しない場合は、ファイルやネットワークを利用することはできません。

バージョンアップ

本製品は、ファームウェア(本製品が動作するための基本ソフトウェア)を更新することができます。最新ファームウェアは、パナソニックのサポートウェブサイトに掲示されます。

フィルタリング（パケットフィルタリング)

ファイアウォールの一種で、フィルター機能を用いて、ネットワークパケットを選択的に転送する方式のことです。適切に設定すると、不要なパケットが外部に転送されるのを防ぎます。

ファイアウォール

インターネットを利用する際のセキュリティの1つ。インターネットからネットワークへの不法な侵入を防ぐ目的で、インターネットとやり取りできるパソコンを制限したり、利用できるインターネットサービスを制限したりします。

ファームウェア

本製品を動作させるプログラムです。本製品ではフラッシュメモリーの中に格納されています。

物理アドレス

MACアドレスと同じ。

つづく

プライベートアドレス (Private address)

主に組織内のLANなど、ネットワークに接続されたときに割り振られたIPアドレスです。プライベートアドレスは申請を行わなくても組織内で自由に割り振ることが可能です。ただし、プライベートアドレスだけでは、インターネット通信ができないためグローバルアドレスを割り振られたルーターなどの機器で中継する必要があります。

プライベートアドレスとサブネットマスクの設定値について

インターネットでは使われないネットワークIDを「プライベートアドレス」と呼び、下の表のようにクラスA、クラスB、クラスCの3段階に分かれています。LANの規模に応じてクラスを選び(たとえば、20台くらいまでのパソコンが接続されたネットワークであればクラスCを選ぶ)、そのクラスのIPアドレスの範囲の中でIPアドレスを設定してください。

クラス	サブネットマスク	プライベートアドレス（この範囲のアドレスは組織内で自由に設定できる）
クラス A	255.　0.　0.　0	10.　0.　0.　1　～　10. 255. 255. 254
クラス B	255. 255.　0.　0	172.　16.　0.　1　～ 172.　31. 255. 254
クラス C	255. 255. 255.　0	192. 168.　0.　1　～ 192. 168. 255. 254

プロキシサーバー

組織内のネットワークとインターネットとの境界で、内部ネットワークの「代理(プロキシ)」として、インターネットとの接続を行うコンピューターやソフトウェアを意味します。内部ネットワークからの特定接続の許可や、外部ネットワークからの不正なアクセスの遮断を行います。回線の負荷を軽減するために、読み込んだファイルを一定時間保存しておくキャッシュ機能をもつプロキシサーバーもあります。

プロトコル (Protocol)

さまざまな情報を種類の異なる複数のコンピューターなどでデータを交換する際の通信規約(約束事)のことです。インターネットでは「TCP/IP」というプロトコルが基盤になっており、そのうえでさらに「http」や「ftp」などの用途別のプロトコルに従って情報の送受信が行われています。

ホスト

各種サービス(たとえば、Eメールの送受信など)に必要な処理のほとんどを行うコンピューターなどの総称として用いられています。

ポート番号

TCPやUDPで、サービス(アプリケーションの種類)を区別するために使われる番号。たとえば、EメールのSMTPは25、HTTPは80が一般的に用いられます。

ポートフォワーディング

静的IPマスカレードと同じ。

つづく

ま

無線LAN

配線を必要としないLAN(ローカルエリアネットワーク)のことです。同一建物内や敷地内など、比較的狭い範囲で電波や赤外線、レーザーなどを使用してネットワークを構築します。

無線LANアダプター

デスクトップパソコンなどを接続して、無線機器として利用することができます。

ら

ルーター
(router)

異なるネットワーク同士を相互接続するネットワーク機器です。異なるネットワーク間の中継点に設置して、ネットワークを介して送信されるデータを適切に目的の場所に届ける役目をもっています。ネットワーク内を流れてきたデータが外部のネットワークあてであれば、ルーターはそのデータを外部に送り出し、ルーターはそのときにどういう経路でデータを配信するかまで判断し、最適なルートに送りだしています。

ルーティング
(routing)

インターネットなどのネットワークにおいてパケットを、正しく目的のノードへ届くように最適な経路を選択・制御すること。

仕　様

【本体】

項　目	仕　様
電　　源	専用ACアダプター　：AC100 V (50 Hz／60 Hz)、DC12 V (品番: PQLV202JP)　DCコード長さ：約1.8 m ACコード長: 約55 cm (別付け)
消費電力	最大約6 W
外形寸法 （幅×高さ×奥行）	W 約204 x H 約36 x D 約140 mm ※アンテナ収容状態
質　　量	約330 g
使用環境	温度 (℃)：　0～40 湿度 (%)：　20～85（ただし、結露なきこと）
WANインターフェース	ポート数：　1 ポート コネクター形状：　8 ピンモジュラージャック（RJ-45） 物理インターフェース：　IEEE 802.3 (10Base-T) IEEE 802.3u (100Base-TX) WAN-LAN間スループット: 最大98 Mbps（SmartBitsによる測定時、IPv4） (当社測定値)　最大72 Mbps（SmartBitsによる測定時、IPv6） 最大85 Mbps (FTP [Static]) 最大71 Mbps (FTP [PPPoE]) 最大40 Mbps (FTP [IPsec]) 最大16 Mbps (FTP [PPTP])
LANインターフェース	ポート数：　4 ポート コネクター形状：　8 ピンモジュラージャック（RJ-45） 物理インターフェース：　IEEE 802.3 (10Base-T) IEEE 802.3u (100Base-TX)
無線インターフェース	■ 無線チップ　Atheros Communications社製 ■ IEEE 802.11a 伝送方式：　OFDM方式、半二重 通信速度 ([規格値] Mbps)：　54／48／36／24／18／12／9／6※ (IEEE 802.11a準拠): Super Aモード対応、 自動フォールバック 周波数範囲 (MHz)：　5170、5190、5210、5230 (中心周波数) チャンネル数：　4 セキュリティ：　WEP64 bit／128 bit／152 bit、SSID、WPA-PSK（TKIP）、WPA2-PSK（AES）、無線ステルス機能(SSID隠ぺい、ANYキーによる接続の許可／拒否)、MACアドレスフィルタリング

つづく

仕　様

項　目	仕　様
無線インターフェース	■ IEEE 802.11b 伝送方式：　DS-SS、半二重 通信速度 ([規格値] Mbps)：　11／5.5／2／1※ (IEEE 802.11b準拠): 自動フォールバック 周波数範囲 (MHz)：　2412～2472 (中心周波数) チャンネル数：　13 セキュリティ：　WEP64 bit／128 bit／152 bit、SSID、WPA-PSK（TKIP)、WPA2-PSK（AES)、無線ステルス機能(SSID隠ぺい、ANYキーによる接続の許可／拒否)、MACアドレスフィルタリング ■ IEEE 802.11g 伝送方式：　OFDM方式 (IEEE 802.11g準拠)／DS-SS方式 (IEEE 802.11b互換)、半二重 通信速度 ([規格値] Mbps)：　54／48／36／24／18／12／9／6※ (IEEE 802.11g準拠): Super Gモード対応、自動フォールバック 11／5.5／2／1※ (IEEE 802.11b互換): 自動フォールバック 周波数範囲 (MHz)：　2412～2472 (中心周波数) チャンネル数：　13 セキュリティ：　WEP64 bit／128 bit／152 bit、WPA-PSK (TKIP)、WPA2-PSK（AES)、SSID、無線ステルス機能(SSID隠ぺい、ANYキーによる接続の許可／拒否)、MACアドレスフィルタリング 通信飛距離:　屋内見通し　約120 m (当社製無線LANアダプターとの通信時) 屋外見通し　約600 m (当社製無線LANアダプターとの通信時) ● 通信距離は環境条件により変化します。鉄筋コンクリートの建物および大型金属製品、電子レンジの近く、盗難防止機器の近くなどでは、通信距離が短くなることがあります。間に障害物(壁や家具、什器)などがある場合、周囲の環境により利用できる範囲は短くなります。 ● IEEE 802.11aの屋外での使用は法律により禁止されています。 ※ 表示の数値は、無線LAN規格の理論上の最大値であり、実際のデータ転送速度を示すものではありません。
ユーザーインターフェース	CLEAR SETTINGボタン：　工場出荷時設定用 状態表示インジケーター POWER：　通電／本体状態表示 WAN：　WANリンク状態表示 PPP:　PPPリンク状態表示 LAN1～LAN4：　イーサネットリンク状態表示 WIRELESS：　無線リンク状態表示
電波障害防止	VCCIクラスB

仕　様

【ソフトウェア】

項　目	仕　様	
ルーター機能	WAN側接続モード	IPv4: PPPoE／DHCP／Static IPv6: ブリッジ、トンネル、6to4、PPPoEIPv4/IPv6、Static
	PPPoEマルチセッション	最大同時セッション数：2
	PPPoE接続／切断	手動接続／常時接続
	RIP	あり（RIPv2）
	RIPng	あり
	DHCPサーバー	あり（128クライアント設定可）
	DNSリレー（DNS代理応答）	あり
	IPパケットフィルタリング	あり（64設定）
	アドレス変換方式	IPマスカレード、静的IPマスカレード (ポートフォワーディング) 、静的NAT
無線機器機能	セキュリティ	WEP(64 bit／128 bit／152 bit)、WPA-PSK(TKIP)/WPA2-PSK(AES)、無線ステルス機能(SSID隠ぺい、ANYキーによる接続の許可／拒否)、MACアドレスフィルタリング
アクセス制限	ID／Password	
ウェブブラウザ設定	あり	
ファームウェア バージョンアップ	あり	
VPN機能	PPTPサーバー (IPv4) IPsec (IPv6)	

保証とアフターサービス（よくお読みください）

修理・お取り扱い・お手入れ
などのご相談は…
まず、お買い上げの販売店へ
お申しつけください

転居や贈答品などでお困りの場合は…

- 修理は、サービス会社・販売会社の「修理ご相談窓口」へ！
- その他のお問い合わせは、「お客様ご相談センター」へ！

■保証書（別添付）

お買い上げ日･販売店名などの記入を必ず確かめ、お買い上げの販売店からお受け取りください。よくお読みのあと、保存してください。

保証期間：お買い上げ日から本体1年間

■補修用性能部品の保有期間

当社は、このカメラコントロールユニット（IPv6／VPN対応無線ルーター）の補修用性能部品を、製造打ち切り後5年保有しています。

注）補修用性能部品とは、その製品の機能を維持するために必要な部品です。

修理を依頼されるとき

「ご使用の前に／困ったときには」の「故障かなと思ったとき」に従ってご確認のあと、直らないときは、まずACコードのプラグを抜いて、お買い上げの販売店へご連絡ください。

- **保証期間中は**
  保証書の規定に従って、お買い上げの販売店が修理をさせていただきますので、恐れ入りますが、製品に保証書を添えてご持参ください。
- **保証期間を過ぎているときは**
  修理すれば使用できる製品については、ご要望により修理させていただきます。下記修理料金の仕組みをご参照のうえ、ご相談ください。
- **修理料金の仕組み**
  修理料金は、技術料・部品代・出張料などで構成されています。

  技術料 は、診断・故障個所の修理および部品交換・調整・修理完了時の点検などの作業にかかる費用です。

  部品代 は、修理に使用した部品および補助材料代です。

  出張料 は、お客様のご依頼により製品のある場所へ技術者を派遣する場合の費用です。

ご連絡いただきたい内容	
製品名	カメラコントロールユニット（IPv6／VPN対応無線ルーター）
品　番	BL-BR30
お買い上げ日	年　　月　　日
故障の状況	できるだけ具体的に

お願い

- 停電などの外部要因により生じたデータの損失ならびに、その他直接、間接の損害につきましては、当社は責任を負えない場合もございますので、あらかじめご了承ください。

本製品は日本国内用です。国外での使用に対するサービスはいたしかねます。

修理に関するご相談

ナショナル・パナソニック　修理ご相談窓口

ナビダイヤル（全国共通番号）　**0570-087-087**

- お客様がおかけになった場所から最寄りの修理ご相談窓口につながります。呼出音の前にNTTより通話料金の目安をお知らせします。
- 携帯電話・PHS等からは最寄りの修理ご相談窓口に直接おかけください。
- 最寄りの修理ご相談窓口は、次ページをご覧ください。

使いかた・お買い物などのご相談

ナショナル・パナソニック　お客様ご相談センター

365日／受付9時～20時

電話　フリーダイヤル　**0120-878-365**（パナは365日）

■携帯電話・PHSでのご利用は…**06-6907-1187**

FAX　フリーダイヤル　**0120-878-236**

Help desk for foreign residents in Japan
〈外国人／海外仕様商品（ツーリスト商品他）等ご相談窓口〉
Tokyo (03) 3256 - 5444　**Osaka** (06) 6645 - 8787
Open : 9:00 - 17:30 (closed on Saturdays / Sundays / national holidays)

保証とアフターサービス（よくお読みください）

ナショナル・パナソニック
修　理　ご　相　談　窓　口

ナビダイヤル（全国共通番号）　0570-087-087

- お客様がおかけになった場所から最寄りの修理ご相談窓口につながります。呼出音の前にNTTより通話料金の目安をお知らせします。
- 携帯電話・PHS等からは最寄りの修理ご相談窓口に直接おかけください。

北海道地区

地区	所在地	電話番号
札幌	札幌市厚別区厚別南2丁目17-7	☎(011)894-1251
旭川	旭川市2条通21丁目左1号	☎(0166)31-6151
帯広	帯広市西19条南1丁目7-11	☎(0155)33-8477
函館	函館市西桔梗589番地241（函館流通卸センター内）	☎(0138)48-6631

東北地区

地区	所在地	電話番号
青森	青森市第二問屋町3-7-10	☎(017)739-9712
秋田	秋田市御所野湯本2丁目1-2	☎(018)826-1600
岩手	盛岡市羽場13地割30-3	☎(019)639-5120
宮城	仙台市宮城野区扇町7-4-18	☎(022)387-1117
山形	山形市平清水1丁目1-75	☎(023)641-8100
福島	福島県安達郡本宮町字南ノ内65	☎(0243)34-1301

首都圏地区

地区	所在地	電話番号
栃木	宇都宮市御幸町194-20	☎(028)689-2555
群馬	高崎市大沢町229-1	☎(027)352-1109
茨城	つくば市花畑2丁目8-1	☎(029)864-8756
埼玉	桶川市赤堀2丁目4-2	☎(048)728-8960
千葉	千葉市中央区星久喜町172	☎(043)208-6034
東京	東京都世田谷区宮坂2丁目26-17	☎(03)5477-9780
山梨	甲府市宝1丁目4-13	☎(055)222-5171
神奈川	横浜市港南区日野5丁目3-16	☎(045)847-9720
新潟	新潟市東明1丁目8-14	☎(025)286-0171

中部地区

地区	所在地	電話番号
石川	石川県石川郡野々市町稲荷3丁目80	☎(076)294-2683
富山	富山市寺島1298	☎(076)432-8705
福井	福井市開発4丁目112	☎(0776)54-5606
長野	松本市大字笹賀7600-7	☎(0263)86-9209
静岡	静岡市西島765	☎(054)287-9000
名古屋	名古屋市瑞穂区塩入町8-10	☎(052)819-0225
岡崎	岡崎市岡町南久保28	☎(0564)55-5719
岐阜	岐阜県本巣郡北方町高屋太子2丁目30	☎(058)323-6010
高山	高山市花岡町3丁目82	☎(0577)33-0613
三重	久居市森町字北谷1920-3	☎(059)255-1380

近畿地区

地区	所在地	電話番号
滋賀	守山市勝部6丁目2-1	☎(077)582-5021
京都	京都市伏見区竹田中川原町71-4	☎(075)672-9636
大阪	大阪市北区本庄西1丁目1-7	☎(06)6359-6225
奈良	大和郡山市筒井町800番地	☎(0743)59-2770
和歌山	和歌山市中島499-1	☎(073)475-2984
兵庫	神戸市中央区琴ノ緒町3丁目2-6	☎(078)272-6645

中国地区

地区	所在地	電話番号
鳥取	鳥取市安長295-1	☎(0857)26-9695
米子	米子市米原4丁目2-33	☎(0859)34-2129
松江	松江市平成町182番地14	☎(0852)23-1128
出雲	出雲市渡橋町416	☎(0853)21-3133
浜田	浜田市下府町327-93	☎(0855)22-6629
岡山	岡山県都窪郡早島町矢尾807	☎(086)292-1162
広島	広島市西区南観音8丁目13-20	☎(082)295-5011
山口	山口市鋳銭司字鋳銭司団地北447-23	☎(083)986-4050

四国地区

地区	所在地	電話番号
香川	高松市勅使町152-2	☎(087)868-9477
徳島	徳島県板野郡北島町鯛浜字かや108	☎(088)698-1125
高知	南国市岡豊町中島331-1	☎(088)866-3142
愛媛	松山市土居田町750-2	☎(089)971-2144

九州地区

地区	所在地	電話番号
福岡	春日市春日公園3丁目48	☎(092)593-9036
佐賀	佐賀市鍋島町大字八戸字上深町3044	☎(0952)26-9151
長崎	長崎市東町1949-1	☎(095)830-1658
大分	大分市萩原4丁目8-35	☎(097)556-3815
宮崎	宮崎市本郷北方字草葉2099-2	☎(0985)63-1213
熊本	熊本市健軍本町12-3	☎(096)367-6067
天草	本渡市港町18-11	☎(0969)22-3125
鹿児島	鹿児島市与次郎1丁目5-33	☎(099)250-5657
大島	名瀬市長浜町10-1	☎(0997)53-5101

沖縄地区

地区	所在地	電話番号
沖縄	浦添市城間4丁目23-11	☎(098)877-1207

所在地、電話番号が変更になることがありますので、あらかじめご了承ください。

0904

さくいん

英　字

ページ
CLEAR SETTINGボタン............17、144
DC INジャック 17
DHCP接続 35
DHCPサーバー機能...............................108
DHCPスタティック 109
DMZ機能 ....87、93
DNSリレー..110
IPsec ....122、134
IPv6 ....44、101、116、150
IPアドレス..
31、44、108、117、150、158、160
IPマスカレード 90
LANジャック 17
MACアドレスフィルタリング 78
MS-CHAP...121
MS-CHAPv2...121
MTUサイズ 111
Ping 134
PPPoE接続................32、39、51、133
PPPoEマルチセッション機能.................59
PPTP ....120、154
SSID..69、71
Static接続.............................37、42、53
UPnP[TM]機能 ....113、145
WANジャック 17

あ

ページ
アドレス変換 81
暗号化......................73、75、121、125
インジケーター................................17、18
インターネット接続..................................56
オプション設定..........................107、116

か

カメラ自動登録機能..................................64
カメラモニター画面..................................26
カメラを使う 63
かんたん設定 19

さ

再起動 ....132、144
サポート...113
仕様...143
詳細設定...23
初期化 ....132、144
ステータス 136
ステートフル・パケット・
インスペクション..........................97、102
ストレートケーブル 7
静的IPマスカレード........................83、89
静的NAT...88
セキュリティ設定..........................95、101
接続設定管理 57

つづく

さくいん

た

ページ
ダイナミックルーティング ....111、118
通信チャンネル..................................69、72
トップページ 19

は

バージョンアップ 129
バックアップ 131
パナソニックのサポートウェブサイト..128
パスワード変更 128
工場出荷時設定一覧.................................165
フィルタリング...............................98、104
フィルタリングログ.................................139
プロキシサーバー 157
プロバイダー登録.............................31、44
ヘルプ...143
ポートフォワーディング ....83、89

ま

みえますねっと設定...................................79
無線設定..69

や

用語解説..170

ら

ログ表示..139
リンクMTUサイズ...................................118

■ 本製品は、外国為替および外国貿易法に定める規制対象貨物（または技術）に該当します。本製品を日本国外へ持ち出す場合は、同法に基づく輸出許可等必要な手続きをお取りください。

This product is a Restricted Product (or contains a Restricted Technology) subject to the Japanese Foreign Exchange and Foreign Trade Law. In case that it is exported or brought out from Japan, you are required to take the necessary procedures, such as obtaining an export license from the Japanese government, in accordance with the Law.

■ 本製品は日本国内用です。国外での使用に対するサービスはいたしかねます。

This product is designed for use in Japan.

Panasonic cannot provide service for this product if used outside Japan.

愛情点検 **長年ご使用のカメラコントロールユニットの点検を！**

こんな症状はありませんか？

- ACアダプターのコードが傷んでいる。
- こげくさい臭いや異常な音がする。
- 内部に水や異物が入った。
- その他の異常や故障がある。

このような症状のときは、使用を中止し、故障や事故防止のため、コンセントからACコードのプラグを抜いて、必ず**販売店に点検を**依頼してください。

便利メモ（おぼえのため、記入されると便利です）

お買い上げ日	年　月　日	品　番	BL-BR30
販売店名	電話　（　　　）　　—		

松下電器産業株式会社
パナソニック コミュニケーションズ株式会社
テレコムカンパニー

〒812-8531　福岡市博多区美野島4丁目1番62号

PSQF1028ZA KK1104RM0